G46392

Technik NEWS

JUNI 1999

DAS PRAXISNAHE NETZWERKMAGAZIN

N° 06

9. JAHRGANG

thema des monats

KERN-TECHNK

NetWare 5 Operating System

CITRIX

Installation des Meta - Frame Client

inhalt

AKTUELL

· TN: Service-CD jetzt im Abo inbegriffen 3

NEWS

· AVM: FRITZ!GSM und FRITZ!Card mit neuen Features 4
· AVM: KEN! bringt die FRITZ!Card ins Netz 5
· AVM: Hochleistungs-ISDN auf acht Kanälen parallel 5
· CS: 8 Port Fiber Optic Switch für Glasfasernetze 6
· ELSA: Gebührenoptimierung mit der LANCOM Office-Router-Serie 6
· Cisco: Access-Plattform für SONET/SDH 7
· Cisco: QoS Policy Manager 7
· Compaq: Enterprise Network Storage Architecture 8
· HP: NetServer mit Intel Pentium III 500 MHz 9
· BinTec: Brick-X21 für WAN-Verbindungen 10
· Compaq: 15 Zoll Flachbildschirm TFT 5000 10
· Novell: Betatest der Cluster Services für NetWare 5 11
· Newsticker 12

THEMA DES MONATS

· Kern-Technik: NetWare 5 Operating System 14
· Novell: NetWare5 Basis der NetWare for Small Business 21
· Citrix MetaFrame, Teil III: Installation des MetaFrame Client 22

HOTLINE

· Microsoft: TCP/IP-Probleme unter Windows NT 4.0, Teil II 30
· ARCserve: Jahr 2000-fähig? 33
· Tobit: Tips der Hotline, Teil 1 34
· ICP: Controller der GDT RP Serie auch ohne CPU-Kühler 36
· Novell: Service-spezifische IP-Portnummern 37
· Microsoft: Tips und Tricks zu Windows NT, Teil I 38
· Neue Patches in der Übersicht: Microsoft und Novell 40
· Tobit, BinTec, AVM und ArcServe Patches in der Übersicht 40
· Empfohlene Computer Associates Updates und Patches 42
· Neue Patches in der Übersicht: Novell Updates und Patches 43
· Neue Patches in der Übersicht: Tobit Updates und Patches 44
· Neue Patches in der Übersicht: Microsoft Updates und Patches 44
· Neue Patches in der Übersicht: Computer Associates 45

PRAXIS

· Das NetWare IPX/SPX Protokoll 46
· Letzte Beta-Phase für Windows 2000 52
· Operation 2000 53
· GroupWise 5.5: Neuerungen in der Administration 54

SEMINARINFOS

· Sommer-Trainings-Camp ´99 60
· Compu-Shack Bookstore 61
· Seminargruppen Übersicht 61

VORSCHAU

· Kostenlose Trials und Datenblätter auf der CS-Homepage 62
· Neue Windows 2000 Kurse 62
· Messen, Roadshows, Termine 63

impressum

Herausgeber: COMPU-SHACK Electronic GmbH, Ringstraße 56-58, 56564 Neuwied

Telefon: 02631/983-0
Telefax: 02631/28100
Electronic Mail: TECHNEWS @ COMPU-SHACK.COM

Redaktion: Heinz Bück, Jörg Marx

Verantwortlich für den Inhalt: Heinz Bück

Technische Leitung: Ulf Wolfsgruber

Erscheinungsweise: monatlich 1 Heft

Bezugsquelle: Bezug über COMPU-SHACK Electronic GmbH Abonnementpreis: 119,- DM + MwSt.

Layout und Titelbild: Marie-Luise Ringma

Lithos: Görres-Druckerei, Koblenz
Druck: Görres-Druckerei, Koblenz
Lektorat: Andrea Briel

Abo-Versand: Wolanski GmbH, Bonn

Reproduktionen aller Art (Fotokopien, Mikrofilm, Erfassung durch Schrifterkennungsprogramme) - auch auszugsweise - nur mit schriftlicher Genehmigung des Herausgebers.

Wir möchten uns nachträglich bei all denen bedanken, die durch die freundliche Zusammenarbeit das Erscheinen dieser Zeitung ermöglicht haben.

Als Informationsquelle dient uns auch das Internet. Wenn Sie speziell über Ihre Erfahrungen referieren möchten, bieten wir Ihnen dies unter der Rubrik "Hotline" an.

Technik NEWS ONLINE

www.compu-shack.com

Selbstverständlich kann COMPU-SHACK die einwandfreie Funktion der vorgestellten Patches und Tips nicht garantieren und übernimmt keinerlei Haftung für eventuell entstehende Schäden.

Patch-CD enthält folgende neue Patches:

NW5SP2.exe
DS411Q.exe
ZW110P2.exe
BM3SP1.exe
MW26SP1.exe
MWINOC7R.exe
MWINOC8O.exe
EXCHNT1.exe
BMTCPE02.exe
BMADM2C.exe
IWSP6A.exe
NWMAC.exe
SP5I386.exe
MAILGATE.exe
DVINFO.exe
PMNW.exe
PMNT.exe
TLD.exe
DAVE-MEX.exe

Service Pack 5 für Windows NT

Mehr für´s Geld

Service-CD jetzt im Abo inbegriffen, doch wir werden teurer

Von Heinz Bück

Technik News hat ihren Leserservice über die Jahre kontinuierlich ausgeweitet. Seit je stand für die Macher des Netzwerkmagazins der praktische Nutzen für die Netzwerker vor Ort ganz oben an. Nach vielen Jahren der Preisstabilität wollen wir jetzt den Abopreis erhöhen. Dafür werden wir den Service aber weiter ausbauen. Die halbjährliche Extra-Service-CD wird Bestandteil des Abonnenments, schon mit der nächsten Ausgabe. Die Patchdatenbank wird ausgebaut. Und zum Erfahrungsaustausch gibt es im Internet die Technik Newsgroup.

Weil wir unseren Leserservice weiter ausbauen wollen, kommen wir nicht umhin, wie andere auch die Preise zu erhöhen. Die Technik News wird teurer. Aber wir bieten jetzt noch mehr für´s Geld. Unsere Service-CD, die zusätzlich zur aktuellen Monats-CD zweimal im Jahr die Standardpatches und langlebigen Updates aufnimmt, wird ab sofort an alle Abonnenten gehen. Sie wird der Juli-Ausgabe bereits beiliegen.

Wir teilen uns das

Viele Leser haben uns gefragt, warum die Service-CD für 19,80 DM extra angeboten wird, und warum sie nicht Teil des Abos wird? Monats-CD und Service-CD helfen schließlich, langes Suchen und Download-Kosten zu sparen. Die Antwort lautet, daß dies lediglich eine Frage der Kosten ist, und wir lange gezögert haben, den Preis zu erhöhen. Ein "Standard-Abo" mit Monats-CD beizubehalten und ein "Abo Plus" mit halbjährlicher Service-CD extra anzubieten, wirft nur zusätzliche Verwaltungsarbeit und unnötige Kosten auf, was die Pflege des Post-Verteilers und den Versand anbetrifft. So haben wir uns entschieden, die beiden Service-CDs zum Preis für eine in das Technik News Abo mit aufzunehmen. Dafür wird das Jahres-Abonnement mit der nächsten Fälligkeit auf 119,- DM angehoben. Wir teilen uns sozusagen die Kosten. Nachbestellungen von Service-CDs müssen aber nach wie vor mit 19,80 DM bezahlt werden.

Wir bieten noch mehr

Unsere Patchdatenbank, die auch über Technik News Online zugänglich ist, soll weiter ausgebaut werden. Der Pflegeaufwand ist jedoch nicht unerheblich. Gleichzeitig muß die Monats-CD immer öfter aufgeräumt werden, um Platz für brandaktuelle Patches und neu hinzukommende Herstellersoftware zu schaffen. Damit gewinnt die Service-CD aber eine immer größere Bedeutung, um die Standardpatches aufzubewahren, die regelmäßig zum Einsatz kommen und langlebiger sind. Sie wird unverzichtbar angesichts der Fülle monatlich neu erscheinender Updates und Software Releases, und gehört konsequenterweise ins Abo.

Um die Bedienerfreundlichkeit zu erhöhen, werden wir die Benutzeroberfläche von Monats-CD und Service-CD verbessern. Sie sollen übersichtlicher werden.

Technik NEWS ONLINE

Wir unterstützen Netzwerker

Wir sind dabei, ein neues Forum für den praktischen Erfahrungsaustausch zu aktuellen Problemen im Netzwerk einzurichten. Zur gegenseitigen Unterstützung können Netzwerker in der Technik Newsgroup auf einer eigenen Leserplattform aktuelle Fragen stellen und Antworten auf besondere Probleme geben und finden. Gleichzeitig sind über unseren Online-Service im Internet Dokumentationen als PDF-Files und kostenlose Demo- oder Trial-CDs abrufbar. Wir streben eine möglichst breite Unterstützung unserer Leser an, getragen von der Philosophie, die Compu-Shack zu einem der größten deutschen Netzwerk-Distributoren gemacht hat, daß Anwendersupport und Partnerunterstützung unumstößliches Prinzip einer kundenbezogenen Value Added Distribution sind.

Von daher hoffen wir auf Ihr Verständnis, wenn Ihre Technik News demnächst teurer wird.

Sie ereichen die Redaktion per E-Mail unter technews@compu-Shack.com.

AVM

Was macht Fritz?

FRITZ!GSM und FRITZ!Card mit neuen Features

Mit FRITZ!GSM offeriert AVM Remote Access, Internet-Zugang, Fax oder Dateitransfer ohne zusätzliche Hardware. AVM weitete die Unterstützung von Mobiltelefonen inzwischen auch auf Nokia aus. FRITZ!Card kommt in der neuesten Version mit Call-by-Call-Unterstützung und TAPI-Support, während „Automatic ISDN" FRITZ! fax, FRITZ! data und FRITZ! vox intelligente Rufnummernerkennung beschert.

Nun können auch Besitzer des Mobiltelefons Nokia 8810 mobiles ISDN, die nahtlose digitale Verbindung zwischen tragbaren Computern und Unternehmensnetzen oder Kommunikationsdiensten über GSM-Mobiltelefone, mit FRITZ!GSM von unterwegs nutzen. Damit ist FRITZ!GSM für Mobiltelefone der Baureihen Siemens S10, SL10, E10, Sony CMD-X2000 und Nokia 8810 verfügbar. Die Unterstützung weiterer datenfähiger Mobiltelefone von Nokia, Ericsson, Bosch und Motorola ist geplant.

FRITZ!GSM

FRITZ!GSM ermöglicht Notebooks auf Basis der GSM-Standards 07.07/07.08 einen schnellen und sicheren Datenaustausch über fax-/datenfähige Mobiltelefone. Mit ISDN/GSM sind schnelle Anwahlzeiten, hohe Übertragungsraten, Sicherheit und „Short-hold-mode" realisierbar. FRITZ!GSM besteht aus der Programm-Suite FRITZ! mitsamt der erforderlichen Treibersoftware. Enthalten sind Module für Telefax, Filetransfer sowie Zugangssoftware für Online-Dienste und Internet. Die Datenverbindung ist sowohl mit digitalen ISDN- als auch mit analogen Gegenstellen möglich. Zusammen mit AVMs NetWAYS/ISDN entfaltet die GSM/ISDN-Verbindung ihre volle Leistungsfähigkeit, mit hoher Geschwindigkeit durch Datenkompression, großer Sicherheit durch D-Kanal-Authentifizierung und Callback sowie geringen Verbindungskosten durch Short-hold-mode.

FRITZ!Card

Mehr Komfort und Ergonomie bei der ISDN-Kommunikation wird die Version 2.08 von FRITZ! bieten. AVM FRITZ!Card Kunden erhalten mit der neuesten Version gleich ein ganzes Paket neuer Features, von der Call-by-Call-Unterstützung bis zum TAPI-Support. Nun lassen sich die Vorwahlrufnummern der bevorzugten Serviceanbieter speichern und bei der Anwahl aus der Datenbank zur Rufnummer hinzufügen. AVM stellt die FRITZ!Software 2.08 wie gewohnt als Update für registrierte Nutzer kostenlos zum Download auf dem AVM Data Call Center bereit.

data, fax, vox und fon

„Automatic ISDN" nennt AVM die neue Funktion der intelligenten Rufnummernerkennung durch die FRITZ!-Module fax, data und vox. Für jede eingehende Rufnummer läßt sich ein spezielles Profil hinterlegen, das eingehende Anrufe individuell bedient. Der Anrufer erhält so nicht mehr nur die Standardnachricht, sondern nun auch eine maßgeschneiderte Antwort. Auf diese Weise können per Faxpolling Telefaxdokumente mit individuellem Inhalt abgerufen oder im Anrufbeantworter persönliche Nachrichten für jeden zu erwartenden Anrufer hinterlegt werden. Auch bei FRITZ!fon, dem jüngsten Modul der FRITZ!-Programmsuite, wurde nochmals nachgelegt. Ermöglicht die Software bereits heute komfortables Telefonieren mit dem PC, so unterstützt die neue Version zukünftig Tonwahl während eines laufenden Gesprächs, die Dreierkonferenz oder auch die Aufzeichnung von Gesprächen mit dem PC. **K.-Nr.0601**

Was macht Fritz im Netz?

AVM KEN! bringt die FRITZ!Card ins Netz

Zugeschnitten auf die Anforderungen im Small Business bringt AVM KEN! Internet, Electronic Mail, Daten, Fax und Sprache an den Arbeitsplatz. In Verbindung mit einem ISDN-PC-Controller bietet die neue AVM-Software eine vollständige Infrastruktur für alle Kommunikationsanforderungen. KEN! sorgt durch eigenen Web- und Mail-Proxy sowie intelligenten Verbindungsaufbau für wirtschaftlichen Betrieb.

KEN! stellt in Windows 95/98 oder Windows NT-Netzen die Applikationsschnittstelle CAPI 2.0 für 16- und 32 Bit CAPI-Anwendungen bereit und unterstützt MSN für eingehende und ausgehende Verbindungen. Ein Server im Netzwerk ist nicht einmal nötig. Zusammen mit einem AVM ISDN-Controller auf einem PC installiert, erhalten alle vernetzten Workstations mit der neuen Software einen Zugang zum ISDN-Basisanschluß. Jeder PC verhält sich so, als wäre eine eigene ISDN-Karte eingebaut. Die kostengünstigste Variante stellt dabei die FRITZ!Card dar. Flexible Infrastrukturen für kleine Büros inklusive Telefonie und Datenkommunikation sind mit den Smart Devices FRITZ!X PC und FRITZ!X USB möglich, die in Verbindung mit KEN! eine Einheit aus Internet-/Mailserver, Telekommunikations-Server und PBX darstellen.

Internet und E-Mail

Für Internet und Electronic Mail genügt ein einziger Zugang zum Provider. Dabei hält KEN! die Kommunikationskosten so niedrig wie möglich. Die Verbindung mit dem Internet erfolgt „on-demand“, also automatisch bei Bedarf. Das Paket enthält einen eigenen FTP- und HTTP-Proxy. Die gesamte Internet-Kommunikation wird über nur einen ISDN-B-Kanal gesteuert. Der integrierte E-Mail-Server basiert auf POP3 sowie SMTP und erlaubt die Zwischenspeicherung von E-Mails. Er ist voll kompatibel zu Clients wie MS Outlook Express oder Netscape Mail.KEN! ist als lokaler E-Mail-Server verwendbar und basiert auf den internationalen Standards CAPI, PPP over ISDN oder PAP/CHAP. Er bietet dynamische IP-Adressen, Datenkompres-sion, Kanalbündelung, IP-Masquerading, Firewall, DNS-Forwarding oder DHCP-Server für die automatische Vergabe von IP-Adressen im Netz. **K.-Nr.0602**

Neue Leistungsklasse

Hochleistungs-ISDN auf acht Kanälen parallel

Mit dem neuen ISDN-PC-Controller C4 erschließt AVM eine neue Leistungsklasse in der ISDN-Datenkommunikation. Speziell auf den Einsatz in Internet-, Daten- und Telekommunikationsservern zugeschnitten, unterstützt die PCI-Einsteckkarte bis zu vier ISDN-Basisanschlüsse. Damit stehen in lokalen Netzwerken acht Datenkanäle für den gleichzeitigen Betrieb zur Verfügung, die in beliebiger Zahl gebündelt genutzt werden können.

Mit seiner besonderen Konzeption bildet der AVM ISDN-Controller C4 die Plattform für Internet Access, Internetworking, Remote Access, Dateitransfer, Fax-, Sprach- und Video-Anwendungen in praktisch allen Netzen, die mehr als zwei Kanäle für ihre Kommunikationsanforderungen benötigen. Ausgerüstet mit einem 233 Megahertz RISC-Prozessor ermöglicht der AVM ISDN-PC-Controller C4 selbst rechenintensivste Anwendungen wie etwa Datenkompression oder den gleichzeitigen Versand von acht Telefaxen mit einer Geschwindigkeit von bis zu 33,6 Kilobit in der Sekunde. Dank CAPI-Interface ist der neue ISDN-Controller mit allen standardkonformen Applikationen unmittelbar einsetzbar. Die Controller-Software ist vollständig konform zum CAPI 2.0 Interface und unterstützt die Betriebssysteme Microsoft Windows NT, Novell NetWare sowie Linux. Für die digitale Datenübertragung stehen alle gebräuchlichen Protokolle zur Verfügung.

Auf acht Kanälen

Die parallele Nutzung aller acht angebotenen Kanäle bedeutet eine kumulierte Bandbreite von 512 Kilobit in der Sekunde. Zusätzlich können Anwendungen Datenkompression nach V.42bis nutzen und damit abhängig von den zu übertragenden Daten ein Vielfaches der physikalischen Übertragungsgeschwindigkeit erreichen. Seine volle Leistungsfähigkeit spielt der ISDN-Controller C4 in der Kommunikation mit analogen Gegenstellen aus: über die übliche Geschwindigkeit von 14.4 Kilobit in der Sekunde hinaus können nun Faxe mit Fax G3F auf bis zu acht Kanälen gleichzeitig in einer Geschwindigkeit von 33.6 Kilobit in der Sekunde gesendet und empfangen werden. Mit der gleichen Geschwindigkeit kann mit analogen Modems vollduplex nach dem Übertragungsstandard V.34 oder mit V.32bis. **K.-Nr.0603**

COMPU-SHACK

Fiber to the desktop

8 Port Fiber Optic Switch für Glasfasernetze

Die Compu-Shack Production rundet ihr Produktportfolio rund um Glasfasernetzwerke ab. „Fiberoptic to the desktop" heißt die Devise. Der neue 8 Port 100Base FX Fiberoptic Switch komplettiert das Angebot und bringt High Performance bis in den Arbeitsplatzbereich. Und auch die kompletten Adapterkartenfamilien für 10, 100 und 1000Mbit/s Ethernet-Netzwerke sind jetzt in Fiberoptik-Versionen auf dem Markt.

Compu-Shack bietet technisch ausgefeilte „Fiber to the desktop-Lösungen" zu einem höchst attraktiven Preis, verbunden mit den Vorteilen eines kundenfreundlichen Supportes. Der 8 Port 100Base FX Fiberoptic Switch steht in einem überzeugenden Preis/Leistungs-Verhältnis. In Ergänzung zu den neuen Fiberoptic-Karten stellt Compu-Shack einen äußerst leistungsfähigen Glasfaser-Switch bereit, der auf Basis der neuen MT-RJ Miniatur-Transceiver Technik entwickelt wurde.
Mit diesem auf der Layer 2 Switching Technologie basierenden Gerät können Sie jetzt komplette Glasfasernetzwerke vom Rechenzentrum bis zum Desktop realisieren.

MT-RJ Anschlußtechnik

Compu-Shack bietet daneben ihre bewährten FDDI-Adapterkarten für Glasfasernetze. Interessant ist dabei vor allem die Flexibilität dieser Produktfamilien bezüglich der angebotenen Anschlußvarianten, die einerseits die Wahl zwischen Multimode- und Monomode-Glasfaserkabel ermöglichen und neuerdings auch den MT-RJ-Stecker neben ST und Duplex SC unterstützen. Die neue MT-RJ Anschlußtechnik erlaubt die Konstruktion von erheblich kostengünstigeren aktiven Infrastrukturkomponenten.
Darüber hinaus werden sehr viel kompaktere Patch-Felder realisierbar. Deshalb wird sich die MT-RJ-Technik als neue Fiberoptic-Anschlußtechnik etablieren.
Über Compu-Shack kann die gesamte Palette an Infrastruktur-Zubehör für MT-RJ bezogen werden. **K.-Nr.0604**

ELSA

Least-Cost-Routing Call by Call

Gebührenoptimierung mit der LANCOM Office-Router-Serie

Die LANCOM Office-Router-Serie von ELSA ist seit neuestem mit einer Least-Cost-Routing-Funktion ausgestattet. Dank LCR sind ELSA LANCOM-Anwender nun in der Lage, im Call-by-Call-Verfahren zu unterschiedlichen Tageszeiten über verschiedene Telefongesellschaften die jeweils günstigsten Tarife zu nutzen.

Das Least-Cost-Routing mit ELSA LANCOM vermittelt die günstigsten Telefontarife und sorgt für erhebliche Kostenersparnisse. Nach Eingabe der Vorwahlnummer, Netzkennzahl, Uhrzeit und Wochentagsinformation ist die LCR-Funktion startklar. Der LANCOM Office-Router übernimmt nach dem Call-by-Call-Verfahren automatisch die vom Anwender gewünschten, kostengünstigen Telefonverbindungen.

Kosten senken

Die LANCOM Office-Router arbeiten hohen Telefonkosten in der Bürokommunikation entgegen. LCR kann für jede Betriebsart der LANCOM Office-Router - ISDN-Router, ELSA LANCAPI und Telefonanlage - genutzt und einzeln eingeschaltet werden. Die Office-Familie besteht derzeit aus den drei Modellen ELSA LANCOM 1000 Office, 1100 Office und 2000 Office. Für bereits ausgelieferte LANCOM-Produkte stellt ELSA unter `www.elsa.de/lancom` Firmware-Updates der Least-Cost-Routing-Funktion zur Verfügung. **K.-Nr.0605**

Access-Plattform für SONET/SDH

Einfache Migration zu „IP-intelligenten“ Netzwerken

Cisco Systems bringt den ISR 3303 auf den Markt, eine neue Access-Plattform mit voller Interoperabilität für Synchronous Optical Network/Synchronous Digital Hierachy. Die SONET/SDH-Lösung eignet sich für Service Provider, um Legacy-Sprachdienste und innovative IP-Dienste auf einer integrierten Plattform mit niedriger Cost-of-Ownership bereitstellen können.

Der Cisco ISR 3303 verfügt über die Routing-Features der Software Cisco IOS sowie den auf Glasfasern basierenden UPSR-Access (Unidirectional Path Switched Ring) eines SONET/SDH Add/Drop Multiplexers. Dadurch kann das Gerät vor allem am Netzwerk-Edge von Service Providern zum Einsatz kommen. Durch die Software Cisco IOS lassen sich mit dem Cisco ISR 3303 neue Services wie Managed Internet Access und native LAN-Services über bestehende Time Division Multiplexer (TDM) anbieten.

Punkt-zu-Netzwerkanwendungen

Durch seine Leistungsmerkmale ist der Cisco ISR 3303 für TDM- und Ethernet-Schnittstellen geeignet. Er unterstützt Punkt-zu-Netzwerkanwendungen mit Breitband-POS (Packet-over-SONET) zur skalierbaren Aufteilung der Datenbandbreite innerhalb eines SONET-Netzwerkes. Im Punkt-zu-Netzwerkbetrieb können Service Provider ihre vorhandene Netzwerk-Infrastruktur weiterverwenden. Der Cisco ISR 3303 ersetzt zwei separate Komponenten, die zuvor zum Zugriff auf SONET-Ringe und zum IP-Routing benötigt wurden. Er verfügt über acht DS1-Ports und acht 10BaseT Ethernet-Ports. **K.-Nr.0606**

Neuer Manager

CiscoAssure: The Quality of Service

Mit dem neuen QoS Policy Manager präsentiert Cisco Systems innerhalb der CiscoAssure Initiative eine Lösung zur Umsetzung von Quality of Service Policies. Sie erkennt Applikationen unternehmensweit und ermöglicht die zentrale Steuerung und automatische Umsetzung von Policies. Damit können Netzwerk-Administratoren die Performance geschäftskritischer Applikationen steuern und schützen.

Im vergangenen Jahr wurde die CiscoAssure Initiative vorgestellt. Sie stellt Produkte und Services für Hochleistungs-Netzwerke bereit, die Applikationen erkennen und unterschiedlich verarbeiten. So ermöglicht CiscoAssure die unternehmensweite Registrierung von Anwendernamen und Adressen, die automatische Verteilung von Policies für netzwerkweite QoS, Security und Sprachdienste sowie die ständige Erweiterung der Internet-Services von Cisco. Mit dem neuen Cisco QoS Policy Manager wurde die zweite Phase der CiscoAssure Initiative jetzt abgeschlossen. Er arbeitet mit den bewährten QoS-Mechanismen der Software IOS für die Cisco LAN/WAN-Switching Komponenten, um QoS Policies schnell zu konfigurieren und zu verteilen.

QoS-Management

Hohe Verfügbarkeit und vorhersagbare Performance geschäftskritischer Applikationen einerseits sowie leistungsfähige Sprach- und Multimedia-Services andererseits setzen eine differenzierte Behandlung des Netzwerkverkehrs voraus. Der Cisco QoS Policy Manager verfügt über einen regelbasierenden Policy Builder sowie die integrierte Validierung von Policies. Der Policy Distribution Manager überträgt die Vorgaben der Policies zu den einzelnen Netzwerkgeräten. Mit einer einfach zu bedienenden grafischen Bedieneroberfläche lassen sich der Netzwerkverkehr klassifizieren und QoS Policies umsetzen. Zu den Software-Releases von Cisco IOS und den Komponenten von Cisco, die mit QoS Policy Manager arbeiten, gehört auch CiscoWorks2000, so daß die Einrichtungszeiten von QoS Policies deutlich verkürzt werden. Da die QoS-Lösung langwierige und fehlerträchtige Konfigurationen in einzelnen Switches und Routern überflüssig macht, lassen sich QoS Policies mit unterschiedlichen Service Leveln der Applikation effizienter umsetzen. **K.-Nr.0607**

Skalierbare SANs

Enterprise Network Storage Architecture

Compaq bringt eine Reihe von neuen Storage Area Network (SAN)-Lösungen und Enterprise Backup Solutions auf den Markt. Das Spektrum der Produkte auf der Basis der Enterprise Network Storage Architecture (ENSA) umfaßt Neuentwicklungen im Bereich Fibre Channel Switch-Technologie, fehlertolerante Software und eine Backup-Lösung mit höherer Kapazität, Skalierbarkeit und Verfügbarkeit. Ergänzt werden die neuen Produkte durch umfangreiche Support-Leistungen von Compaq Services.

Compaq bietet für heterogene Plattformen und für nahezu alle maßgeblichen Betriebssysteme hohe Verfügbarkeit in SAN-Umgebungen sowie neue Backup-Lösungen für Windows NT, Novell NetWare, Tru64 UNIX und OpenVMS. Mit neuen Produkten baut Compaq ihr Lösungsspektrum auf der Basis der Enterprise Network Storage Architecture (ENSA) weiter aus.

Enterprise Backup Solution

Die Compaq Enterprise Backup Solution wurde speziell für komplexe, geschäftskritische Unternehmensumgebungen auf Basis von Windows NT oder Novell NetWare konzipiert. Sie bildet eine integrierte SAN Backup-Lösung, die Hardware von Compaq einschließlich Fibre Channel Host-Adaptern, Hubs, Bandlaufwerks-Controllern und DLT-Tape-Libraries mit Software führender Hersteller kombiniert. Die Enterprise Backup Solution unterstützt Fibre Channel Bandbreiten von 100 MB/s für kleiner werdende Backup-Zeitfenster und stellt eine Architektur bereit, mit der sich parallele Backups von mehreren Servern zu einzelnen oder mehreren DLT-Libraries problemlos realisieren lassen. Um dem wachsenden Kapazitätsbedarf der Unternehmen optimal zu entsprechen, hat Compaq ihre Enterprise Backup Solution mit einer besonders leistungsstarken Tape-Library ausgestattet. Die TL895 unterstützt bis zu sieben DLT-Laufwerke und maximal 96 Bandkassetten mit bis zu 6,7 TB Speicherkapazität. In Kombination mit der optimierten Performance und Verwaltungsfunktionalität entsteht eine Lösung, die höchsten Anforderungen in komplexen Umgebungen mit Windows NT und NetWare gerecht wird.

Storage Arrays

Die StorageWorks Systeme Enterprise Storage Array 12000 (ESA12000) und RAID Array 8000 (RA8000) wurden für anspruchsvolle unternehmensweite Applikationen ausgelegt und bieten Funktionen für zentralisierte Verwaltung, hohe Verfügbarkeit, überlegene Leistungsfähigkeit und Skalierbarkeit in offenen Systemumgebungen. Diese Systeme sind jetzt mit Fibre Channel Switched Fabrics erhältlich. Skalierfähige SANs können mit StorageWorks RA8000 und ESA12000 Lösungen sowie neuen 8- und 16-Port Fibre Channel Switches konfiguriert werden, die den Aufbau mehrerer tausend Verbindungen unterstützen. Bis zu 32 Switches mit acht parallelen Verbindungen zwischen jedem Switch-Paar sind möglich.

Fehlertolerante Systeme

Mit der StorageWorks Data Replication Manager Software und den Switched Fabric SANs mit StorageWorks RA8000 oder ESA12000 läßt sich ein kontinuierlicher, ausfallsicherer Systembetrieb gewährleisten. Die RAID-Controller-basierte Software unterstützt die Online-Replikation von geschäftskritischen Daten in Echtzeit an lokalen und dezentralen Standorten. Mit der StorageWorks Data Replication Manager Software lassen sich Daten mit Fibre Channel-Geschwindigkeiten von 100 MB/s zwischen Standorten replizieren, die bis zu zehn Kilometer voneinander entfernt sind. Das Wiederherstellen der Datenbestände ist nur noch eine Frage weniger Minuten. Der StorageWorks Data Replication Manager ist für die Betriebssysteme Windows NT, Tru64 UNIX und OpenVMS verfügbar. **K.-Nr.0608**

Integratives Management

NetServer mit Intel Pentium III 500 MHz

Hewlett-Packard erweitert ihre PC-Server-Familie um Modelle mit Intel Pentium III 500 MHz-Prozessor. Der neue Intel Chip steht für die HP NetServer-Linien LC3, LPr und LH3 sowie für die neuen Rechner der HP NetServer E-Serie zur Verfügung. Die neuen HP Server sind zudem mit einer Reihe innovativer Management-Lösungen ausgestattet.

Die PC-Server-Reihen der HP NetServer Familie warten mit Neuerungen auf. Sie sind neuerdings nicht allein mit Intel Pentium III 500 MHz-Prozessor zu haben, HP stellt außerdem für jeden PC-Server kostenlos die PC-Management-Software HP TopTools zur Verfügung. Sie erlaubt es, daß nun auch Fremdkomponenten von IBM und Compaq integriert und über eine Managementkonsole verwaltet werden können. Weiterhin unterstützt bei der neuen HP NetServer-Generation das für ein Single Node geltende HP OpenView ManageX/SE 4.0 künftig Novell NetWare 3.12 und 4.1x.

Fault Notifier

Die integrierten HP TopTools verfügen jetzt über den Fault Notifier. Er ermöglicht den HP NetServer-Systemen, Fehlermeldungen selbständig und gezielt weiterzuleiten. Der Administrator braucht die Schlüsselkomponenten seines Systems nicht mehr manuell zu überwachen, um Ausfallzeiten zu verhindern. Statt dessen überprüfen die HP TopTools die Server-Hardware fortwährend auf mögliche Fehlerquellen. Der Fault Notifier warnt automatisch per E-Mail das HP Response Center und den Systemadministrator, wenn wichtige Hardware-Komponenten versagen. Sie können so früher korrigierend eingreifen und Ausfallzeit vermeiden oder reduzieren. HP TopTools sind in allen HP NetServer Systemen integriert. Das neue Fault Notifier-Modul ist kostenlos mit den HP SupportPacks sowie anderen Support-Vereinbarungen für alle HP NetServer Systeme erhältlich.

Management

Darüber hinaus erweitert HP die Unterstützung von HP OpenView ManageX/SE 4.0. Die Management-Lösung unterstützt neben Microsoft Windows NT nun auch Novell NetWare 3.12 und 4.1x. Neue ManageX/SE-Verfahren zur Erhöhung der Betriebszeit ergänzen die HP TopTools-Lösung. So lassen sich beispielsweise Parameter wie die Prozessor-Temperatur und überschüssige Energieversorgung überwachen. Sie erlauben IT-Managern, Reaktionenroutinen auf vorhersehbare Systemfehler festzulegen. ManageX/SE 4.0 ist ab Anfang März lieferbar.

NetServer Familie

Die HP NetServer Familie besteht aus zwei PC-Server-Reihen sowie einer komplett vorkonfigurierten Internet-Lösung, dem HP NetServer Webmaster. Die HP NetServer E-Serie richtet sich an kleine Betriebe und Workgroups und ist damit für Netzwerkumgebungen gedacht, die nur wenig oder kein IT-Management haben. Die L-Serie reicht vom Server für kleine und mittlere Arbeitsgruppen, dem HP NetServer LC3, über den Abteilungsserver HP NetServer LH3 bis zum Highend-Server für große Unternehmen, dem HP NetServer LXr 8000 sowie dem 8-Wege-System LXr Pro8. Allen HP NetServern liegt die NetServer Navigator CD-ROM bei, die einfache Konfigurations-, Installations- und Servermanagementtools bereithält.

Für erhöhte Zuverlässigkeit der HP NetServer sorgt eine neue Lösung bei den HP Surestore DDS-Bandlaufwerken. Auf Knopfdruck lassen sich nach einem Systemabsturz verloren gegangene Daten wiederherstellen. **K.-Nr.0609**

BINTEC

Weit und fern

Brick-X21 für WAN-Verbindungen

Mit der BIANCA/Brick X21 bietet BinTec Communications jetzt eine kostengünstige Lösung für den Einsatz in Weitverkehrsnetzen. Der kleine Hardware-Router ist fest bestückt mit einem X.21-Interface und einen Doppel-ISDN-S$_0$-Interface. LAN-seitig ist durch den integrierten 10/100 Mbit/s Autosensing-Controller eine Ankopplung an Ethernet und Fast Ethernet möglich.

Die Brick X21 wird vielfältigsten Leistungsanforderungen gerecht. Mit dem Leased Line / ISDN-Multiprotokoll-Router für TCP/IP und IPX können Daten, Bilder und Fax-Nachrichten übertragen werden. Optional lassen sich die Protokolle X.25 und Frame Relay einbinden. Dabei können die vorhandenen ISDN-BRI-Anschlüsse entweder als Einwahl-Ports oder als Backup-Ports für die X.21-Verbindung genutzt werden. Die breit angelegte Kommunikations-Architektur BIANCA, die BinTec Advanced Network Communication Architecture, bietet über unterschiedliche Rechnerplattformen hinweg unter Windows 3.x, Windows 95, Windows NT und UNIX eine neue Dimension an Leistungsmerkmalen und Konfigurationmöglichkeiten.

Easy Administration

Der administrative Aufwand wird nicht nur über automatische Steuermechanismen, sondern auch über eine problemlose Autokonfiguration des ISDN-Anschlusses sehr gering gehalten. Ein leicht bedienbares, integriertes Setup-Tool zur Konfiguration und ein einfaches Systemmanagement mit SNMP-Standardtools bzw. mitgelieferter Benutzeroberfläche DIME sorgen für einen reibungslosen Bedienkomfort. Wie von BinTec Routern gewohnt, bietet auch die Brick X21 alle notwendigen Sicherheits-Features. Über die integrierten Firewall-Mechanismen, die SAFERNET-Technologie, wird der Netzzugang gesichert. Ebenso findet der Kunde in der Software-Ausstattung wirkungsvolle Sicherheitsfunktionen wie PAP- und CHAP-Authentisierung und Network Address Translation. **K.-Nr.0510**

COMPAQ

Ich leg mich flach

15 Zoll Flachbildschirm TFT 5000

Mit dem neuen TFT5000 baut Compaq ihr umfangreiches Monitor-Portfolio weiter aus. Der TFT5000 erweitert das bestehende Compaq Angebot an Flachbildschirmen um ein Modell, das in puncto Flexibilität einzigartig im Markt ist. Der Bildschirm bietet maximale Performance und verfügt über ein äußerst flexibles Display, das auf die Anforderungen unterschiedlichster Geschäftsumgebungen zugeschnitten ist.

Flachbildschirm-Technologie überzeugt aufgrund ihrer besonderen Bildqualität und ihres platzsparenden Designs gerade in beengten Arbeitsplatzumgebungen. Der TFT5000 bietet eine 15-Zoll Weitwinkel-Bildfläche mit SuperBright-Technologie und eine Farbpalette von bis zu 16,7 Millionen Farben. Der ‚Pivot Mode' ermöglicht es dem Anwender, den Bildschirm um 90 Grad zu drehen, also von der gewohnten Querformat- in die Hochformat-Ansicht zu wechseln. Darüber hinaus erlaubt der höhenverstellbare Sockel, den Bildschirm in der Höhe so zu variieren, bis die optimale Sichthöhe für den Anwender erreicht ist. Kleinere Auflösungen werden durch modernste Algorithmen problemlos an die gesamte Bildschirmgröße angepaßt. Der TFT5000 wird mit automatischem Setup, mit dem Kontrast und Schärfe eingestellt werden können, ausgeliefert. Die Compaq Flachbildschirme verbrauchen weniger Strom als gewöhnliche CRT-Monitore, geben weniger Hitze ab und benötigen weniger Kühlung, was zu geringeren Energiekosten führt. Alle Compaq Monitore sind TCO '95 und MPR II zertifiziert. Darüber hinaus sind sie Energy Star kompatibel, CE Mark zertifiziert und erfüllen die Kriterien für PC 98. Alle Compaq Monitore werden mit einer umfassenden Standard-garantie ausgeliefert. Dazu gehören drei Jahre Garantie inklusive Vor-Ort-Service im ersten Jahr.
K.-Nr.0511

Cluster-Test

Betatest der Novell Cluster Services für NetWare 5

Die Betaversion der verzeichnisbasierenden Novell Cluster Services für NetWare 5 ist verfügbar. Die neue Lösung sorgt für hohe Verfügbarkeit beim Zugriff auf geschäftskritische Daten in transaktionsorientierten Anwendungen wie etwa beim Internet-Shopping im Bereich E-Commerce. Der neue Cluster nutzt die Novell Directory Services zur Verwaltung aller Ressourcen, die zu einem Cluster zusammengeschaltet sind.

Die Novell Cluster Services for NetWare 5 befinden sich zur Zeit in der Betatestphase. In Verbindung mit NetWare 5 ermöglichen sie zuverlässige Geschäftstransaktionen sowie den Zugriff auf die Netzwerkressourcen von jedem Ort aus. Die Shared Disk Array-Technologie der Novell Cluster Services reduziert Ausfallzeiten durch die Möglichkeit, daß andere Server innerhalb eines Clusters die Dienste und Applikationen eines ausgefallenen Servers übernehmen können. Bei Störungen werden die dort laufenden Anwendungen automatisch auf einem anderen Server des Clusters gestartet. Gleichzeitig werden die Anwender, die bisher am ausgefallenen Server angemeldet waren, unmerklich auf andere Server umgeleitet.

NDS Integration

Die Novell Cluster Services nutzen die Eigenschaften der Novell Directory Services. Sie speichern alle Konfigurationsinformationen des Clusters innerhalb der Verzeichnisdatenbank. So greifen sie im Fehlerfall nicht auf Batch-Prozeduren zurück, um eine Reaktion auf einen Serverausfall auszulösen, sondern auf die in den NDS gespeicherten und verteilten Informationen zu Fehlerszenarien. Auf diese Weise sind die Informationen durch die Verzeichnisse allen Servern innerhalb des Clusters bekannt. Des weiteren beinhalten die Novell Cluster Services einen Multi-Node-Support und unterstützen jetzt mehr als zwei Knoten in einem Cluster.

Auf der diesjährigen Brainshare in Utah führte Novell zwei Cluster mit jeweils 12 Knoten vor, die auf Servern von Hewlett-Packard und Compaq unter NetWare 5 arbeiteten. Für eine einfache Administration sorgt Novells Java-basierendes Console One-Verwaltungstool.

Fan-In, Fan-Out

Das sogenannte Application Fan-Out erlaubt die Verteilung von Applikationen eines ausgefallenen Servers auf ein beliebige Zahl anderer Server innerhalb des Clusters. Umgekehrt lassen sich beim Application Fan-In geschäftskritische Applikationen bei mehreren Server-Abends gleichzeitig auf eine kleinere Anzahl von Servern zusammenziehen. So ist auch bei schwerwiegenden Serverausfällen die Sicherheit der kritischen Applikationen gewährleistet.

Das Auto-Reconnect sorgt für eine automatische, transparente Migration von IP-basierenden Clients eines ausgefallenen Servers auf die weiterhin verfügbaren Server des Clusters.

Die Betaversion steht zum Download unter `http://support.novell.com/beta/public/` bereit. **K.-Nr.0513**

Vierte Phase

Multiservices für Campus und WAN

Cisco Systems stellte neue Komponenten aus der vierten Phase ihrer fünfstufigen Strategie zur Integration von Daten, Sprache und Video vor. Die aktuellen Neuheiten verbessern vor allem die Campus-Telefonie, die WAN-Interoperabilität und den Multiservice Customer Support von Cisco. Die Multiservice-Funktionen ermöglichen die integrierte Daten-, Sprach- und Video-Kommunikation über das gesamte Netzwerk. So erhalten auch kleine Unternehmen und ausgelagerte Standorte betriebsbereite Lösungen, mit denen sich die Migration zur unternehmensweiten IP-Telefonie und Campus/WAN-Interoperabilität realisieren läßt. Zu den neuen Multiservice-Produkten und -Features gehören der neue Cisco CallManager 2.2 sowie Kommunikations-Systeme zur LAN-Telefonie in kleinen Unternehmen und Außenstellen, der Virtual Switch Controller VSC 2700 für die ATM Switch Router der Reihe Catalyst 8500, verbesserte Video-Funktionen des Cisco MC3810 Access Concentrator sowie Verbesserungen am Voice over Frame Relay und am Voice over Internet Protocol für die Gateways der Reihen Cisco 2600, 3600 und MC3810.

K.-Nr.0514

Windows 2000 kompatibel

ISDN-Controller auf Windows 2000 CD

Die CAPI-Treiber der AVM ISDN-Controller sind bereits Windows 2000-konform und werden von Microsoft auf der aktuellen Beta 3 Version des neuen Betriebssystems mit ausgeliefert. Die Treiber arbeiten nach dem Win32 Driver Model (WDM), das die automatische Erkennung der Hardware bei der Installation ermöglicht. Neben dem CAPI-Treiber werden bei allen plug-and-play-fähigen ISDN-Controllern gleichzeitig die AVM NDIS WAN CAPI-Treiber für Internetzugang und RAS installiert. Alle AVM CAPI-Treiber unterstützen die Schnittstellen 16- und 32bit DLL, 32 Bit Device Driver Level sowie CAPI 2.0 und 1.1. Sie stehen zur Verfügung für die aktiven Controller B1, B1 PCI, USB und PCMCIA, die FRITZ!Cards Classic, PCI, PnP, USB und PCMCIA sowie für die Primärmultiplex-Controller T1 und T1-B. Für FRITZ!Card-Nutzer ist AVMs Ankündigung der neuen ISDN TAPI-Services von besonderem Interesse. Denn damit wird es möglich, alle TAPI-basierten Telekommunikationsanwendungen mit der FRITZ!Card über ISDN zu nutzen. Die direkte Anwahl von Gesprächspartnern erfolgt mit der Microsoft Wählhilfe, aber auch jede andere auf TAPI basierende Software kann benutzt werden. **K.-Nr.0516**

Für 90 Tage

Kostenfreier Telefon-Support

3Com erweitert ihr Service-Angebot rund um die SuperStack II und OfficeConnect Produktfamilien für kleine und mittelständische Betriebe. Ab sofort werden fast alle Produkte dieser Familien mit einem Anrecht auf kostenfreien Telefon-Support für 90 Tage ausgeliefert. Die Registrierung hierfür erfolgt nach dem Kauf auf einer speziellen Webseite.
Der offerierte Telefon-Support garantiert einen Rückruf spätestens am nächsten Werktag und erleichtert kleineren Unternehmen den Einstieg in Netzwerkumgebungen. Die Customer Service Organisation von 3Com bietet individuell angepaßte Service-Pakete.
So ist bei Vertragskunden ein Erst-Rückruf innerhalb der ersten Stunde garantiert und auch kürzeste Reparatur- oder Austauschzeiten lassen sich in sensiblen Bereichen wie Banken oder Versicherungen vertraglich vereinbaren. **K.-Nr.0515**

Im neuen Gewand

Nachfolger mit neuen Features

Mit neuer Speicherarchitektur kommt der bewährte Cisco1600-R Router auf den Markt. Nun arbeiten die Modelle Cisco1601-R und 1603-R mit RAM Memory. Die Trennung des Speicherplatzes der IOS Software und der separaten Memory-Kapazität für den Betrieb des Feature Packs ermöglichen eine enorme Performance-Steigerung. Die R-Modelle bieten 30% mehr Performance für speicherintensive Applikationen wie Datenkompression, Encryption-Software oder Firewall Feature Sets. Außerdem erlaubt der neue 1600-R ein Software Upgrade über jede Schnittstelle des Routers während des laufenden Netzwerkbetriebs. Ein Aufrüsten ist also leicht gemacht. Die Anzahl der zur Verfügung stehenden IOS Software Feature Packs ist zwar mit der Anzahl der original Cisco1600 Router identisch, jedoch sind die Feature Packs der neuen und alten Routergeneration nicht untereinander austauschbar. Die

Software für den neuen Cisco 1600-R ist im Gegensatz zum bisherigen Paket komprimiert und lagert sich im Betrieb vom Flash auf den RAM-Speicher aus. Außerdem beinhaltet die neue IP only IOS Release 12.0T für die Cisco1600-R Geräte nun auch Network Address Translation, das OSPF Routing Protokoll und RADIUS. **K.-Nr.0517**

Hochverfügbarkeit

StandbyServer für NetWare 5

Der VINCA StandbyServer für NetWare 5 ist da. Die einfach zu installierende, hardware-unabhängige Software gewährleistet die Verfügbarkeit von kritischen Netzwerkressourcen. Die neuartige Spiegelungstechnologie setzt auf Gerätetreiberebene bei einzelnen I/O Anfragen an, um die Synchronisierung von Daten zwischen den Cluster Servern aufrechtzuerhalten. Die Spiegelung selbst erfolgt über eine separate, dedizierte Serververbindung. Dafür sind keine speziellen Netzwerkkarten oder Kabel nötig. Die Datensynchronisation erfolgt, ohne daß zusätzlicher Traffic im Netzwerk generiert wird. Der gesamte Vorgang ist benutzerdefiniert, so daß der Systemadministrator Ausfallschutzverfahren definieren kann, die optimal auf die Systemumgebung abgestimmt sind. Zusätzlich bietet VINCA mit einem Value Pack einen einjährigen Maintenance- und Supportvertrag an, mit aktuellen Releases, Patches oder Upgrades auf einer monatlichen CD und Supportberechtigung für eine kostenfreie Hotline-Telefonnummer rund um die Uhr. VINCA bietet die Möglichkeit, eines kostenlosen Downloades des StandbyServers unter `www.vinca.com` als Vollversion mit einem Time-Out von 30 Tagen. Entsprechende Vollizenzen können danach überinstalliert werden, ohne die Konfiguration neu zu erstellen. **K.-Nr.0518**

Router Management Labs

Utilities für Jahr-2000-fähige Routernetze

Nortel Networks macht ab sofort die Utilities des Router Management Labs (RML) für alle Interessenten online verfügbar. Damit wird Anbietern von Telekommunikationsdiensten und Unternehmen die Möglichkeit gegeben, große Routernetze schnell und effizient aufzubauen, aufzurüsten und zu verwalten. Die Konfigurationstools und Supportangebote des RML, die unter `www.nortelnetworks.com/rml` abgerufen werden können, stehen kostenlos zur Verfügung. Mit den Netzwerkmanagement-Tools lassen sich von einer zentralen Stelle aus Dateien für die Konfiguration von Routern auf Flash-Cards erstellen und anpassen, die dann direkt in die BayRS-Router eingesetzt werden können. Im Online-Angebot des RML finden Netzoperatoren Werkzeuge, mit denen sie ihr Routernetz effektiv und rechtzeitig Jahr-2000-fähig machen können. **K.-Nr.0519**

Mit deutscher Software

Multilinguale CD für Netzwerkkarten

3Com liefert die Netzwerkkarten ihrer EtherLink XL- und Fast EtherLink XL-Produktfamilien (3C90x) ab sofort mit einer komfortablen Treiber-CD in 11 Sprachen aus. Dank der grafischen Benutzeroberfläche der CD, einem browser-basierten Benutzerhandbuch, Diagnostik-Tools und umfangreichen Dokumentationen ist die Installation der 3Com Netzwerkkarten noch einfacher und auch für Netzwerklaien problemlos durchzuführen. Die neue EtherCD XL in der Version 4.01 unterstützt neben der deutschen Sprache auch Chinesisch, Japanisch, Spanisch, Französisch, Schwedisch, Niederländisch, Italienisch, Koreanisch, Portugiesisch und natürlich Englisch. Der CD liegt ab sofort eine gedruckte, mehrsprachige Kurzanleitung bei. **K.-Nr.0520**

Für jeden etwas

Desktop Management und Groupware

Novell gibt die weltweite Verfügbarkeit von Z.E.N.works 1.1 in Englisch, Portugiesisch, Französisch, Italienisch, Deutsch und Spanisch bekannt. Z.E.N.works 1.1 bietet netzwerkweite Software Distribution und verzeichnisbasiertes Desktop Management über die NDS für Netzwerk-PCs und Thin Clients. Mit Check 2000 hilft Z.E.N.works Y2K-Probleme auf Desktops zu beheben, auf der Ebene des BIOS, des Betriebssystems, der Applikationen, Daten und des Datenaustausch.
Gleichzeitig wurde die Verfügbarkeit von GroupWise 5.5 for Unix für alle lizenzierten Kunden von GroupWise 5.x bekanntgegeben. GroupWise 5.5 for Unix stellt den GroupWise Post Office Agent (POA) und den Message Transfer Agent (MTA) für Solaris SPARC Umgebungen bereit und wurde für heterogene Netzwerke optimiert. Das UNIX Post Office kooperiert mit den GroupWise Post Offices unter NetWare 4.x, NetWare 5.x, und Win dows NT. Die neue Version ist unter `www.novell.com/download` zu finden. **K.-Nr.0521**

KERN-TECHNIK

NetWare 5

Operating System 5

Von Gerhard Wingender

Bei der NetWare 5 wurde der Kernel des NetWare Betriebssystems komplett überarbeitet. Wir sind in die Tiefen vorgedrungen und liefert Ihnen interessante Einblicke in die Kern-Technik bei NetWare 5.

Wenngleich die grafische Benutzeroberfläche für den Server in der NetWare 5 am augenfälligsten ist, so hat doch gerade der Kernel des Betriebssystems weitreichende Veränderungen erfahren. Viele neue Features wie die NCP-Protokollunabhängigkeit sind hinzugekommen. Gleichzeitig hat die Unterstützung für Virtual Memory in den NetWare Kernel Einzug gehalten. Der Administrator hat inzwischen die Möglichkeit, NLMs in speziellen Speicherbereichen zu laden. Wir wollen einmal unter die Oberfläche schauen und in die Tiefen vordringen.

NCP-unabhängig

Ein neues Feature in NetWare 5 betrifft den OS Loader selbst. Neben einigen anderen Veränderungen ist die Eingabe des Kommandos `LOAD` vor dem Namen eines NetWare Loadable Modules (NLM) nicht mehr erforderlich. Um z.B. das Monitorprogramm zu starten, geben Sie an der Server Konsole einfach nur noch `MONITOR` ein.

Das Betriebssystem NetWare 5 ist im Bezug auf das NetWare Core Protokoll (NCP) protokollunabhängig. Das heißt, daß es NCP-Anfragen beantworten kann, die über IP, IPX, UDP oder eine Kombination daraus gestellt werden. Um festzustellen, welche Protokolle in welcher Reihenfolge geladen sind, stehen unter NetWare 5 eine ganze Reihe Konsole-Kommandos und SET-Parameter zur Verfügung. Zu den NCP-spezifischen Kommandos gehören:

```
NCP STATS
NCP ADDRESSES
NCP TRACE
NCP DUMP
```

NCP Adressen

Um zum Beispiel zu ermitteln, welche IPX-, TXP- und UDP-Adressen in welcher Reihenfolge geladen sind, geben Sie an der Server Konsole `NCP ADDRESSES` ein. Wenn Sie dabei feststellen, daß das Laden nicht in der von Ihnen gewünschten Reihenfolge durchgeführt wird, können Sie dies wie folgt ändern: Starten Sie den `MONITOR` und wählen Sie den Menüpunkt `Server Parameters`. Dort wählen Sie `NCP` und bestätigen bei `NCP Protocol Preferences` mit `Enter`. Jetzt können Sie die Reihenfolge, in der die Protokolle verwendet werden sollen eintragen. Die Informationen werden in der Konfigurationsdatei des Servers gespeichert und bei jedem Neustart des Servers automatisch verwendet.

NCP STATS

Das Kommando `NCP STATS` zeigt Ihnen die Anzahl der NCP Requests, die durch das Betriebssystem bis zu diesem Zeitpunkt verarbeitet wurden. Die Zahlen neben den Feldern `ProcessNCPPacket Requests` und `ProcessNCPPacketWith Length` geben die Anzahl der NCP Requests durch das IPX- und IP-Protokoll sowie CLIB an. Der Wert `NCPPacketReceiveHandler` zeigt die Anzahl der NCP Requests durch das IP X-Protokoll. Mit dem Kommando `NCP STATS RESET` können diese Werte zurückgesetzt werden.

NCP TRACE

Mit NCP TRACE können Sie sich die eingehenden NCP Anfrage auf dem Bildschirm des Servers ansehen. Die Syntax für den Befehl lautet `NCP TRACE ON` zum Einschalten, bzw. `NCP TRACE OFF` zum Abschalten des Trace. Die Anzeige des Trace erfolgt auf einem eigenen NCP Trace-Bildschirm. Möchten Sie den Trace für eine spätere Analyse speichern, ist dies über das Kommando `NCP TRACE ON <Dateiname>` möglich. Die Datei mit dem Trace finden Sie dann in der Root von Volume SYS.

NCP DUMP

Über `NCP DUMP <Dateiname>` können Sie sich ansehen, wie die NCPs derzeit implementiert sind, und wie oft sie aufgerufen werden. Diese Option ist aber wohl mehr für den Entwickler gedacht, denn während der `NCP TRACE` mit „normalen“ NetWare-Kenntnissen lesbar ist, benötigt man für `NCP DUMP` schon eine umfangreichere Erklärung, was es mit den Zahlenkolonnen auf sich hat.

Virtual Memory

Mit NetWare 5 hat bekanntlich auch die Unterstützung für Virtual Memory in den NetWare Kernel Einzug gehalten. Was bedeutet dies in der Praxis? Wenn Sie in den Server physikalisch 64 MB eingebaut hatten, war dies in früheren Versionen der maximale Speicher, auf den der Server zum Laden von Applikationen und NLMs zurückgreifen konnte. Mit Virtual Memory kann der Server einige Datenbereiche aus dem Hauptspeicher entfernen und auf der Platte zwischenspeichern. In der Standardeinstellung wird dafür zunächst eine 2 MB große Swap-Datei in der Root des Volumes `SYS` angelegt. Abhängig vom benötigten Hauptspeicher wird die Größe der Datei nun ständig angepaßt. Ein Caching der Swap-Dateien findet dabei übrigens nicht statt.

Swap-Dateien

Der Virtual Memory Mechanismus läßt sich über entsprechende Kommandos konfigurieren. So kann der Administrator ein anderes Volume zum Speichern der Swap-Datei definieren, z.B. aus Performance-Gründen das am wenigsten benutzte Volume. Auch kann er die Anzahl der verwendeten Swap-Dateien erhöhen. Eine Übersicht der verfügbaren Befehle sowie eine kurze Erklärung dazu liefert die Eingabe von `HELP SWAP` an der Konsole des Servers (vgl. Abb. 1).

Basiskomponenten

Das Virtual Memory Modell besteht aus drei Basiskomponenten: Primä-

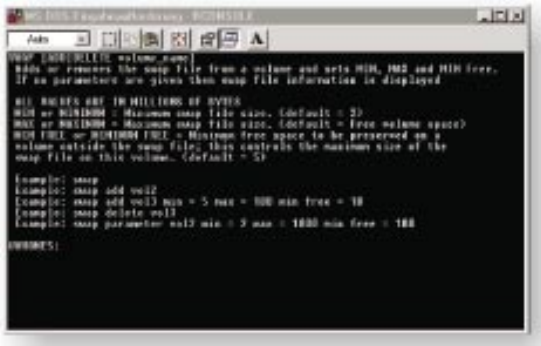


Abb. 1: SWAP HELP zeipt die verfügbaren Befehle zum Virtual Memory an

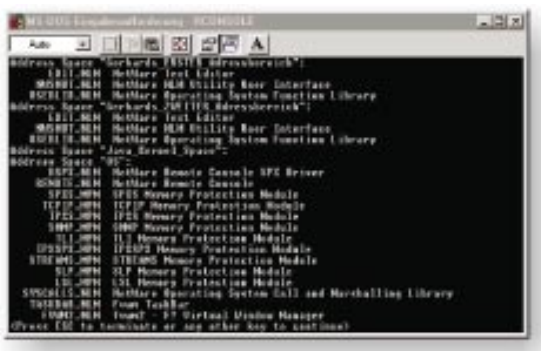


Abb. 2: Anzeige der Adreßbereiche mit geladenen NLMs

rer Speicher, Sekundärer Speicher und Swap-Datei. Der primäre Speicher ist der tatsächlich im Server verfügbare Hauptspeicher. Der sekundäre Speicher ist die Größe des durch laufende Programme belegten Speichers in der Swap-Datei. Der Clou des Betriebssystems ist, daß es nun zu entscheiden hat, wie diese beiden Speicherbereiche so effizient zu verwalten sind, daß es zu einer optimalen Performance und Speicherauslastung führt. Aus Performance-Gründen sollten Sie aber immer darauf achten, daß der sekundäre Speicher maximal zweimal so groß ist wie der primäre Speicher.

Um festzustellen, wie das Virtual Memory auf dem Server konfiguriert werden kann, geben Sie `MONITOR !H` ein. Durch den Parameter `!H` zeigt der Monitor alle versteckten SET-Parameter an. Dann wählen Sie im Menüpunkt `Server Parameter` die Kategorie `Memory`. Doch Achtung: Gerade bei den versteckten SET-Parametern ist höchste Vorsicht geboten. Verändern Sie Einstellungen nur dann, wenn Sie wirklich sicher sind, was Sie tun!

Memory Protection

In NetWare 5 hat der Administrator die Möglichkeit, NLMs in speziellen Speicherbereichen zu laden. Egal welche Abstürze ein NLM in diesem Speicherbereich generiert, kann dies dem Speicherbereich des Betriebssystems und somit dem Kernel nichts anhaben. Zur Ausnutzung dieses Features stehen verschiedene Befehle zur Verfügung.

Adreßbereich

`PROTECTED [RESTART] NLM_Name [address space=name]<Enter>` dient dem Laden eines NLM in einem geschützten Bereich. Über den Parameter `RESTART` kann der Adreßbereich als restart-fähig markiert werden und über den Parameter `address space=` der für diesen Adreßbereich zu verwendende Name. Die Syntax `PROTECTED RESTART EDIT ADDRESS SPACE=TECHNIKNEWS` zum Beispiel lädt den Editor in einen Adreßbereich mit dem Namen `TECHNIKNEWS` und markiert diesen als restart-fähig.

Mit dem Befehl `PROTECTION [[[NO] RESTART] Name des Adreßbereichs]` kann das Flag `restart` für den angegebenen Speicherbereich nachträglich gesetzt oder entfernt werden. Wenn Sie nur `PROTECTION` eingeben, erhalten Sie eine Liste der derzeit vorhandenen Adreßbereiche, sowie die darin ausgeführten Programme (vgl. Abb. 3). Durch die Eingabe von `MODULES` erhalten Sie eine Liste aller geladenen Programme mit der Angabe des jeweils verwendeten Speicherbereichs.

Laden und Entladen

Alternativ können Sie das Laden auch mit dem Befehl `LOAD` durchführen. So lädt der Befehl `LOAD address space=TECHNIKNEWS CLIB` die CLIB in den Adreßbereich `TECHNIKNEWS`. Demzufolge mußte auch der Befehl `UNLOAD` verändert werden, damit das NLM aus dem richtigen Adreßbereich entladen wird. Die korrekte Syntax lautet `UNLOAD ADDRESS SPACE=AdreßbereichsName NLMName`. Der Befehl `UNLOAD ADDRESS SPACE=TECHNIKNEWS CLIB`" würde also die zuvor geladene CLIB wieder entladen. Laden Sie Modules durch eine NCF-Datei, können Sie auch diese Module schützen. Dazu verwenden Sie den Befehl `PROTECT [NCF Dateiname]`. Es werden alle durch die NCF-Datei geladenen NLMs in einem eigenen Speicherbereich ausgeführt.

Server-Konfiguration

Bezüglich der Speicherung von Informationen, die bisher vor allem in den Dateien `AUTOEXEC.NCF` und `STARTUP.NCF` zu finden waren, geht NetWare 5 nun einen anderen Weg. Die Informationen über die Konfiguration des Servers, SET-Parameter sowie andere interne Informationen werden in einer hierarchischen Datenbank in Baumstruktur gespeichert.

Configuration File

Die Datei mit dem Namen `SERVCFG.000` befindet sich auf der DOS-Partition im Verzeichnis `C:\NWSERVER`, sowie im Verzeichnis `SYS:SYSTEM`. Grundsätzlich werden alle Informationen zur Konfiguration zunächst aus der Konfigurationsdatei und dann aus den Dateien `*.NCF` gelesen. Ganz verzichten können Sie auf die Dateien `*.NCF` aber nicht. Denn zum einen sind sie aus Kompatibilitätsgründen vorhanden, und zum anderen sind die Informationen über zu

ladende Treiber offensichtlich auch nicht in der Konfigurationsdatei enthalten. Der Versuch, den Server ohne STARTUP.NCF zu starten, scheiterte. Der Plattentreiber wurde nicht geladen und ohne Plattentreiber keine Volumes. Änderungen an den SET-Parametern werden allerdings direkt in die Konfigurationsdatei geschrieben und brauchen nicht mehr in die AUTOEXEC.NCF Datei übernommen zu werden. Damit Sie die aktuelle Konfiguration des Servers besser überprüfen können, stehen Ihnen bei NetWare 5 folgende Kommandos zur Verfügung.

Display Environment

Das Kommando DISPLAY ENVIRONMENT zeigt Ihnen die aktuellen Suchpfade des Servers sowie die aktuell gültigen Einstellungen der SET-Parameter auf dem Server an. Zur besseren Darstellung werden die SET-Parameter in Weiß und die jeweiligen Einstellungen in Gelb dargestellt. (vgl. Abb. 3). Allerdings bekommen Sie über diesen Befehl nur die Parameter angezeigt, die nicht als hidden gekennzeichnet sind. Informationen zu versteckten Parametern bekommen Sie nur über das Monitor NLM (siehe oben).

Display Modified Environment

Eine Funktion, die wir uns schon seit NetWare 3 wünschen, ist die Möglichkeit, alle veränderten SET-Parameter anzuzeigen. Geben Sie den Befehl DISPLAY MODIFIED ENVIRONMENT ein, so erhalten Sie eine Liste der veränderten Parameter mit den jeweils aktuellen sowie den Default-Werten. (vgl. Abb. 4)

Reset Environment

Ein weiteres tolles Feature ist der Befehl RESET ENVIRONMENT. Nach Eingabe dieser Kommandos bekommen Sie alle veränderten Parameter nacheinander angezeigt und können dann entscheiden, ob Sie den einzelnen Wert auf den Standardwert zurücksetzen möchten oder nicht. Alternativ können Sie auch direkt alle modifizierten Werte auf den Default zurücksetzen.

Save Environment

Insbesondere für den Techniker, aber auch zur Dokumentation des Servers ist der Befehl SAVE ENVIRONMENT <Dateiname> interessant. Mit Hilfe dieses Kommandos können Sie alle aktuellen Environment-Einstellungen des Servers in eine Datei schreiben. Wenn Sie nichts anderes angeben, finden Sie diese Datei danach in der Root von Volume SYS. Sie enthält neben den aktuellen Einstellungen der 295 SET-Parameter auch Angaben über die möglichen Einstellungen sowie die Standardeinstellung.

Save Modified Environment

Der Befehl Save Modified Environment entspricht dem oben beschriebenen Kommando. Allerdings werden in diesem Fall nur die Informationen über die veränderten Parameter in der Datei gespeichert.

Console One

Bekanntlich enthält NetWare 5 erstmals eine grafische Benutzeroberfläche für den Server. Obwohl Sie ihn laut Dokumentation bereits mit 64 MB auf einem Pentium Prozessor betreiben können, sollte er für die grafischen Tools über mindestens 128 MB und einen PII 266 verfügen. Ansonsten werden Sie von der Geschwindigkeit sehr enttäuscht sein.

Screen Switching

Das grafische Administrationstool Console One schreibt seinen Bildschirminhalt nach 15 Minuten Inaktivität automatisch auf die Festplatte. Das führt dazu, daß es beim

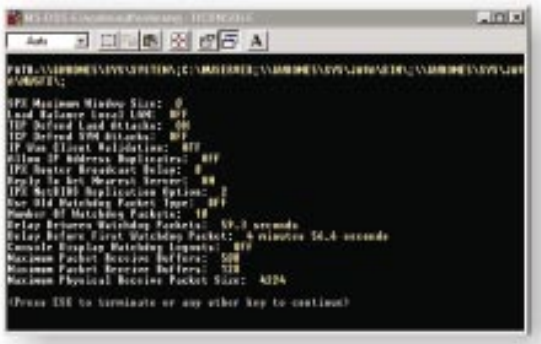


Abb. 3: DISPLAY ENVIRONMENT

Wechseln durch die Server-Bildschirme mit der Tastenkombination [ALT - ESC] zu einer Verzögerung von einigen Sekunden kommt, wenn der Console One Bildschirm aufgerufen wird. Die Verzögerung wird durch das Laden der Daten von der Platte verursacht. Um dies zu vermeiden, sollten Sie stets die Tastenkombination [CRTL-ESC] verwenden und damit den gewünschten Schirm direkt aufrufen.

GUI am Server

Normalerweise wird die grafische Benutzeroberfläche beim Starten des Servers automatisch geladen. Möchten Sie dies ändern, gehen Sie wie folgt vor. Geben Sie an der Konsole des Servers NWCONFIG ein. LOAD ist wie gesagt nicht mehr erforderlich. Wählen den Menüpunkt Edit Autoexec.ncf und setzen vor den Befehl STARTX.NCF ein #. Möchten Sie dagegen neben der Xwindows-Oberfläche auch direkt das grafische Administrationstool Console One laden, fügen Sie den Befehl C1START.NCF hinter das Kommando STARTX.NCF ein.

Konsolen-Kommandos

Wie Sie bereits erkennen konnten, wurden sehr viele Konsole-Befehle ergänzt, erweitert oder auch verän-

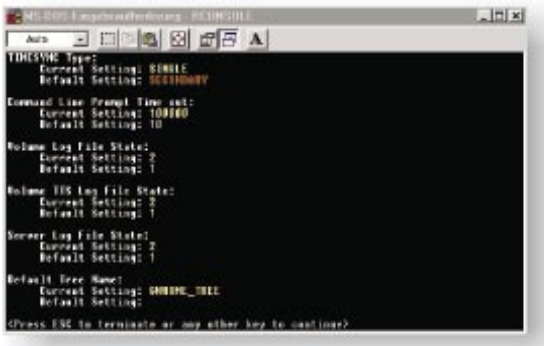


Abb. 4: DISPLAY MODIFIED ENVIRONMENT

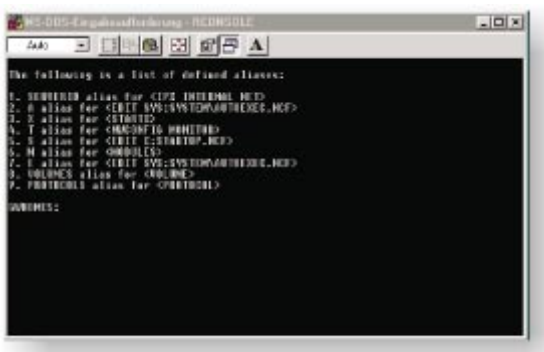


Abb. 5: ALIAS hilft bei langen Befehlen

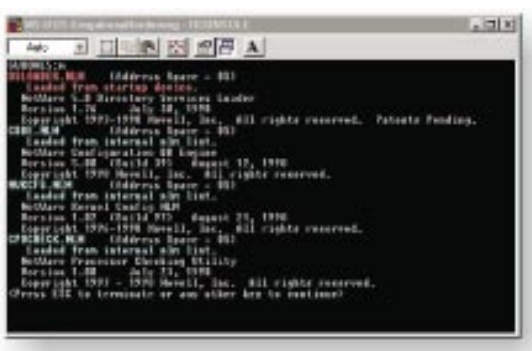


Abb. 6: MODULES zeigt die NLMs in verschiedenen Farben an.

dert. An dieser Stelle möchten wir uns einigen Befehlen zuwenden, die zwar teilweise schon mit der NetWare 4 verfügbar waren, aber erstaunlicherweise noch immer nicht jedem bekannt sind.

Hilfen

Wenn Sie an der Konsole des Servers den Befehl HELP eingeben, erhalten Sie eine Liste aller verfügbaren Kommandos. Über HELP <Kommando > erhalten Sie weitere Hilfe zum entsprechenden Befehl. Es lohnt sich, einfach mal mit dem Kommando zu spielen und nachzusehen, was der Server so alles bietet.

Alias

Alias ist zwar kein neuer Befehl, aber die Funktionalität wurde in NetWare 5 nochmals stark erweitert. Mittels ALIAS können Sie für NetWare-Befehle, die sich teilweise recht schwer merken lassen, andere oder kürzere Namen vergeben. Wenn Sie den Befehl an der Konsole eingeben, erhalten Sie eine Liste der aktuellen ALIAS- Befehle. Den Kommandos VOLUME, PROTOCOL, MODULES und IPX INTERNAL NET wurden bereits im Rahmen der Installation andere Namen zugewiesen. (vgl. Abb. 5). Die Alias-Namen werden in der Konfigurationsdatei des Servers gespeichert und stehen somit auch nach einem Neustart wieder zur Verfügung. Allerdings können Sie einem Alias-Namen immer nur einen Befehl zuweisen.

Der Versuch, einem Alias einen anderen bereits vergebenen Alias zuzuweisen, wird beim Aufruf mit der Fehlermeldung Unknown Command quittiert. Ansonsten sind den Abkürzungen keine Grenzen gesetzt. So können Sie z.B. das Laden des Monitors abkürzen, indem Sie den Befehl ALIAS MO MONITOR eingeben. Zukünftig können Sie damit den Monitor durch die Eingabe von MO starten. Oder sie geben ALIAS A EDIT SYS:SYSTEM\ AUTOEXEC.NCF ein und können ab dann durch ein schlichtes A den Editor mit der Datei AUTOEXEC.NCF starten. Genauso können Sie natürlich auch den Aufruf einer NCF-Datei abkürzen.

Fragezeichen

Über den Befehl ? kann das Laden eines NLMs gesteuert werden. Wenn Sie z.B. in einer NCF-Datei den Befehl ?MONITOR eintragen, erscheint beim Aufruf der NCF-Datei die Anzeige Monitor ?. Sie können jetzt mit n das Laden des Monitors verhindern, oder mit y ausführen lassen. Wenn Sie keine Taste drücken, wird der Monitor nach 10 Sekunden automatisch geladen. Dieser Timeout von 10 Sekunden kann über den SET-Parameter Command Line Prompt Time Out in den Grenzen von 0 bis 4294967295 (>100 Jahre) beliebig verändert werden.

Drei-Tasten-Befehl

Sollten Sie einmal in die Verlegenheit kommen, daß sich die Konsole des Servers aufgehangen hat und Sie nicht mehr auf den Konsolen-Prompt zurückkommen, können Sie den Server mit der Tastenkombination [CTRL+ALT+ESC] runterfahren. Es erscheint ein Menü mit den beiden folgenden Optionen:

1. Down the File Server and Exit to DOS.
2. Cancel the Volume Mount.

Mit [ESC] kommen Sie aus dem Menü wieder heraus, mit 1 fahren Sie den Server nach einer Sicherheitsabfrage herunter und mit 2 können Sie das Mounten eines Volumes abbrechen, wenn Ihnen dieses zu lange dauert.

Modules

Über den Befehl MODULES können Sie sich wie auch in den früheren NetWare-Versionen die geladenen NLMs ansehen. Dieser Befehl ist bereits standardmäßig durch den Alias M abgekürzt. Bei Modules fallen zwei Dinge auf. Zum einen wird nun bei jedem NLM der Adreßbereich, in dem er geladen wurde, angezeigt. Zum anderen erfolgt die Anzeige der NLMs bunt (vgl. Abb.6). Die verwendeten Farben entsprechen weitgehend

Blau	Blaue NLMs wurden von einer festen internen Liste geladen, die beim Ausführen von SERVER.EXE aufgerufen wird. (z.B. NetWare Kernel Config NLM; NWKCFG.NLM)
Rot	Rote NLMs sind ebenfalls in die SERVER.EXE eingebunden. Sie werden von der Start-Partition des Servers (z.B. C:\NWSERVER) geladen. Ein Beispiel für diese NLM-Gruppe stellt die Datei DSLOADER.NLM (der Directory Services Loader) dar.
Lila	Hier handelt es sich um NLMs, die beim Starten des Servers automatisch von anderen NLMs nachgeladen werden. Dies ist vor allem beim Starten des Servers zu beobachten, denn bei der Anzeige durch den Befehl Modules erscheint diese Farbe nicht mehr. Nach dem Starten läßt sich dies leicht mit dem RSPX.NLM testen. Der automatisch nachgeladene REMOTE.NLM erscheint in lila, aber bei der späteren Anzeige über Modules erscheint er in weiß.
Weiß	Diese NLMs wurden vom der Konfigurationsdatei des Servers, aus irgendeiner NCF-Datei (z.B. AUTOEXEC.NCF, STARTUP.NCF), oder von der Konsole des Servers geladen.
Gelb	Gelb werden in der Regel Informationen dargestellt, die Symbolinformationen der geladenen Module betreffen.
Grün	Informationen über die NLMs, die gerade geladen werden, sind in grüner Farbe dargestellt. So werden Sie z.B. häufiger die grüne Meldung „NLMmodulname does not have any XDC data“ sehen. Diese Meldung erscheint, wenn der Multiprozessor-Kernel prüft, ob der NLM multiprozessorfähig ist. Wenn dies nicht der Fall ist, wird diese Meldung angezeigt und der NLM läuft unabhängig davon, wieviele Prozessoren er hat, im Single-Prozessor-Modus.

Tab. 1: Bedeutung der Farben beim Laden von NLMs

jenen, in denen die entsprechenden NLMs beim Starten des Servers angezeigt werden. Die Bedeutung der Farben ist in Tabelle 1 dargestellt.

Loading Stages

Schauen wir noch etwas tiefer in das Betriebssystem der NetWare 5 hinein, so werden wir feststellen, daß es aus mehreren Teilen besteht, dem Loader, dem Server und den Stages

Loader

Der sogenannte Loader läßt sich in `START.EXE` und `LOADER.EXE` aufteilen. Die `START.EXE` ist der 16 Bit Teil, der die CPU in den 32 Bit Modus wechseln läßt und dann die `LOADER.EXE` startet. Die `LOADER.EXE` wiederum stellt dann das Interrupt Subsystem sowie Teile des Debuggers zur Verfügung.

Server

Der Server besteht zum einen aus dem `SERVER.NLM` und zum anderen aus sogenannten `bound-in-NLMs`. Das `SERVER.NLM` stellt Funktionen wie `Scheduling`, `Memory Allocation` oder `NLM Loading` zur Verfügung, während die `bound-in-NLMs` sich jeweils um Spezialaufgaben kümmern, z.B. das `CPUCHECK.NLM`, das `NCP.NLM` oder das `FileSYS.NLM`.

32 Stages

Im Rahmen sogenannter `Stages` werden weitere Teile des Betriebssystems geladen. Dabei wird zwischen den `Kernel-Stages K` und `0` bis `5` und den `User-Stages 6` bis `31` unterschieden. Neben der Stage `K`, die als `Pre-0-Stage` bezeichnet wird, werden also beim Starten des Servers 32 Stages durchlaufen. Während der Stage `K` lädt NetWare die Konfigurationsdatenbank. In ihr stehen alle Informationen darüber, was in welcher Stage geladen werden soll. Die Tabelle 2 zeigt die einzelnen Stages und gibt Beispiele zu den NLMs, die in der entsprechenden Phase geladen werden. Intern läuft das Starten eines Servers nach der Eingabe von `SERVER.EXE` nach diesem Schema ab. Zu `Stages` gibt es eine Reihe von Befehlen, mit denen Sie dies nachvollziehen können (vgl. Tab. 2, auf der nächsten Seite).

`LIST STAGE <Nr>`	Dieser Befehl zeigt die NLMs an, die in der jeweiligen Stage geladen werden. Um also zu sehen, welche NLMs in Stage 0 geladen werden, verwenden Sie die Syntax `LIST STAGE 0`.
`LOADSTAGE <Nr>`	Über den Befehl `LOADSTAGE` können Sie die einzelnen Stages bei Bedarf von Hand laden. Mit der Syntax `LOADSTAGE 3` laden Sie dem nach alle Komponenten aus der Stage 3.
`LOADSTAGE ALL`	Dieses Kommando lädt alle noch nicht geladenen Stages.

Server manuell starten

Aus Support-Gründen kann es bekanntlich erforderlich sein, den Server zunächst ohne Startdateien hochzufahren, um danach schrittweise weiter vorzugehen. Bei NetWare 4 haben Sie ihn dazu mit dem Parameter -NS gestartet und anschließend alle in der AUTOEXEC.NCF enthaltenen Befehle manuell eingegeben. Bei NetWare 5 müssen Sie etwas anders vorgehen. Wenn Sie den Server durch die Eingabe von SERVER -NS starten, werden zunächst nur die Stages K und 0 geladen. Wenn der Server läuft, können Sie die STARTUP.NCF Datei von Hand laden, durch Eingabe von STARTUP an der Konsole des Servers, und dann nach Bedarf die einzelnen Stages durch die Eingabe von <LOADSTAGE Nr> starten. Den bei NetWare 4 durch SERVER -NS erreichten Zustand des Servers rufen Sie bei NetWare 5 durch Starten mit SERVER -NS, manuelles Aufrufen von STARTUP.NCF und anschließender Eingabe von LOADSTAGE 1 hervor. Wenn Sie häufiger damit zu tun haben, sollten Sie sich also zwei NCF-Datei anlegen, die den Server in den Zustand -NS und -NA bringen.

1.	Ausführen von START.EXE und LOADER.EXE
2.	Laden von SERVER.NLM
3.	Laden von Bound-In-NLMs
4.	Ausführen von Stage K
5.	Ausführen von Stage 0
6.	STARTUP.NCF laden
7.	Ausführen von Stage 1
8.	Volume SYS mounten
9.	Ausführen Stage 2
10.	Ausführen Stage 3
11.	Name Space laden
12.	Ausführen Stage 4
13.	AUTOEXEC.NCF laden
14.	Ausführen Stage 5
15.	Ausführen der User-Stages

Tab. 2: Abfolge der einzelnen Stages und der geladenen NLMs nach der Eingabe von SERVER.EXE.

Achtung!
Beachten Sie, daß Sie die einzelnen Stages zwar manuell laden können, ein „Rückwärtsgang“ aber nicht verfügbar ist. Wenn Sie also bei Stage 4 sind und zurück zu Stage 3 möchten, müssen Sie den Server neu starten. Sollten Sie zufällig eines der In-Bound-NLMs entladen haben, können Sie dieses mit dem Befehl LOAD nicht mehr laden. Zum Laden eines In-Bound-NLM ist dem Namen des NLMs ein * voranzusetzen. Wenn Sie also das CPUCHECK.NLM entladen haben, führt ein LOAD CPUCHECK zur Meldung Unable to find load file. Mit der Syntax LOAD *CPUCHECK haben Sie beim Laden des NLMs den gewünschten Erfolg.

Weitere Tips und Tricks:

MONITOR.NLM
Im Menüpunkt Server-Parameter können Sie die SET-Parameter über die Taste [F3] in eine Datei schreiben lassen.

JAVA
Der Befehl JAVA -SHOW zeigt alle laufenden Java-Programme an. Über JAVA -KILLALL können alle laufenden Java-Programme beendet werden.

CDROM
Die „alten“ CDROM-Befehle sind nicht mehr verfügbar. Wenn Sie das CDROM.NLM laden, wird die CD über die NetWare Storage Services angesprochen. Die CD wird automatisch als Volume gemounted, es sind keine weiteren Befehle mehr erforderlich. Sollten Sie aus irgendeinem Grund noch mit dem alten CDROM.NLM arbeiten wollen, können Sie es über LOAD CDINST.NLM laden und mit den alten Kommandos verwenden.

BOOT$LOG.ERR
Fehlermeldungen beim Starten des Servers oder auch danach werden in der Datei BOOT$LOG.ERR eingetragen. Sie finden diese im Verzeichnis SYS:SYSTEM.

CFGFILES.CFG
Die Datei CFGFILES.CFG im Verzeichnis SYS:SYSTEM enthält eine Liste aller *.CFG-Dateien.

SERVER -NL
Um den Server ohne das grafische Logo zu starten, rufen Sie SERVER.EXE mit dem Parameter „-NL“ auf. Diese Änderung wird in der NetWare-Konfigurationsdatei abgespeichert. Nach einem Neustart wird der Server also wieder ohne Logo starten. Um das Logo wieder einzuschalten starten Sie den Server mittels SERVER -L.

Unload NLM
Wenn Sie den Befehl ALIAS U UNLOAD eingegeben haben, können Sie sich das Entladen von NLMs einfach machen. Die Eingabe von U MONITOR entlädt z.B. den Monitor.

In-Bound-NLMs
Alle In-Bound-NLMs lassen sich durch die Eingabe von LOAD *NLM <Name> von Hand laden.

Fazit

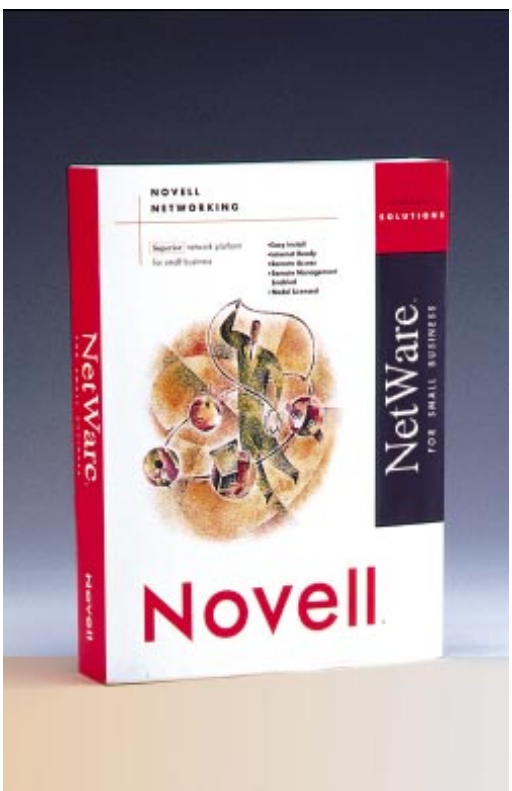
Auch wenn auf den ersten Blick vor allem die grafische Oberfläche als Neuerung am Server auffällt, gibt es doch eine große Anzahl von Veränderungen, viele auch, die im Rahmen diese Artikels gar nicht dargestellt werden konnten. Wir können jedem nur raten, NetWare 5 zu installieren und selbst einmal in Tiefen zu schauen. Wir wollten Ihnen dazu einige Anregungen geben.

Small Business

Im 3. Quartal wird NetWare5 Basis der NetWare for Small Business

Die NetWare for Small Business 4.2 erfreut sich offensichtlich großer Beliebtheit. Im 3. Quartal 1999 wird NetWare5 das Basisprodukt für NetWare for Small Business sein. Beta-Versionen sind schon Ende des 2. Kalenderquartals abrufbar. Wie sehen die Upgrade- und Lizenzierungsmöglichkeiten aus?

Das große Plus der NetWare vor Small Business liegt sicherlich darin, daß alle Komponenten des Komplettpakets sich mit geringstem Aufwand aktivieren lassen. Von der Serverinstallation bis zur Antiviren-Software müssen keine wirklich technischen Fachkenntnisse vorhanden sein, wenngleich man wissen sollte, ob alle Hardwarekomponenten erkannt und richtig aktiviert wurden.



Alles drin

Die NetWare for Small Business beinhaltet eine stattliche Anzahl von Produkten, angefangen bei der NetWare 4.2 (4.11 + Service Packs), GroupWise 5.2, dem BorderManager FastCache bis hin zur Tobit FaxWare 5 und dem Internet Connection Wizard. Die Network Associates Virus Protection, NetObjects Fusion, ZEN Starter Pack 1.0, ManageWise NMA und Netscape FastTrack Server for NetWare kommen hinzu. Network Address Translation, NIAS (MPR & Connect), Netscape Communicator 4.04, Novell SBackup, NAL 2.6 und Oracle 8 sind ebenfalls inbegriffen. Zusätzlichen Funktionen werden im 3. Quartal mit der NetWare5 hinzukommen: Pure IP, die Java Engine, der Multiprozessorkern, aber auch Speicherschutz und Virtueller Speicher.

Lizenzfragen

Vorteile bringt die Novell Lizenzierung insoweit, als man schon mit 1er statt 5er Lizenzen erweitern kann. Es gibt Lizenzerweiterungen der NetWare for Small Business für 1, 5 und 25 Arbeitsplätze. Hierbei handelt es sich um so genannte “User Connection Licenses”. Kunden, die diesen Sommer noch die NetWare for Small Business 4.2 kaufen, werden jedoch keine “kostenlosen” Upgrades mehr erhalten, sondern sollen mit der Produktfreigabe der Small Business auf NetWare5 ein preisgünstiges Angebot über den Fachhandel erwerben können. Novell begründet ihre Entscheidung mit Veränderungen im amerikanischen Steuerrecht.

Neue Standorte

Da mit NetWare for Small Business sogenannte Cross-Upgrade, d.h. Upgrades von NetWare Lite, Personal NetWare, Microsoft NT-Server, Microsoft Small Business Server, Artisoft Lantastic, Banyan Vines, etc. möglich sind und diese keine zur NetWare for Small Business konforme Umgebung voraussetzen, kann das Upgrade auch auf einem neuen System eingesetzt werden.

Bekanntermaßen brauchen NetWare-Versionen älter als NetWare 3.12 allemal ein Update auf eine neuere Version, um im Jahr 2000 lauffähig zu sein.

Im Gegensatz zu Microsoft unterstützt Novell alle gängigen Clients, also zusätzlich zu den weit verbreiteten Systemen wie Windows 95/98 oder Windows NT auch Macintosh und OS/2.

Info-Channels

Beta-Versionen NetWare for Small Business auf Basis der NetWare5 sind Ende des 2. Kalenderquartals unter `support.novell.com / beta` abrufbar.

Weitere Informationen finden Sie unter `www.novell.com / year2000`, weitere Details unter `sup port.novell.com / advan tage` inklusive eines White-Paper-Vergleichs mit Microsoft.

THIN CLIENT

Citrix MetaFrame

Teil III: Installation des MetaFrame Client

Von Hardy Schlinck

Unabhängig vom Betriebssystem des Clients oder dem verwendeten Protokoll schafft Citrix MetaFrame über den entfernten Zugriff auf Server- und Host-Applikationen die Verbindung neuer Welten.

Im ersten Beitrag haben wir uns mit den Grundlagen auseinandergesetzt und geklärt, was eigentlich unter dem Begriff Thin Client/Server Computing zu verstehen ist. Der zweite Teil beschäftigte sich mit der eigentlichen Installation der Software, namentlich dem MetaFrame Server. In diesem dritten Teil werden wir die Client-Software auf den Workstations installieren, zum einen mit dem Konfigurationsprogramm ICA Client Creator, zum anderen über eine bestehende Netzwerkverbindung.

Generell kann man unterscheiden zwischen lokalen Verbindungen mit Zugriff des Client auf den Server des lokalen Netzwerkes und einer Verbindung zwischen zwei LANs über ISDN- oder analoge Router-Technologie. In beiden Fällen verwendet man eins der Protokolle IPX/SPX/NetBEUI oder TCP/IP. Weiterhin ist es möglich, den Server-Zugriff mit Hilfe von Standardmodems einzurichten. Als Protokoll kommt diesmal die Einstellung `async` zum Einsatz. Wenn sich im System eine ISDN-Karte befindet, die über einen WAN-NDIS-Miniport- oder CAPI-Port-Treiber verfügt, so kann auch diese Verbindungsart genutzt werden. Generell wird die Hardware unterstützt, die für den Microsoft Windows Terminal Server zertifiziert ist. Wenn Sie als Transportprotokoll `asnyc` ausgewählt haben, sind weitere Konfigurationen erforderlich, die sich auf die Installation des Modems und dessen Einstellung beziehen.

Client-Software installieren

Nachdem die entsprechende Konfiguration des Connection-Profiles durchgeführt wurde (vgl. Teil II), müssen Sie die Client-Software auf den entsprechenden Workstations installieren. Um diese Aufgabe zu erfüllen, gibt es zwei Möglichkeiten: die Installation über das Konfigurationsprogramm ICA Client Creator oder über eine bestehende Netzwerkverbindung.

ICA Client Creator

Das Konfigurationsprogramm ICA Client Creator ermöglicht es, Installationsdisketten für die verschiedenen Client-Betriebssysteme anzufertigen. Gestartet wird der ICA Client Creator mit Hilfe der Taskbar unter dem Punkt `Programs / MetaFrame Tools / ICA Client Creator`. Anschließend öffnet sich ein Fenster, in dem Sie entscheiden müssen, für welches Betriebssystem die Client-Disketten erstellt werden sollen.

Über Netzwerkverbindung

Während der Installation des MetaFrame Client über eine bestehende Netzwerkverbindung werden die Dateien für den Client auf die Festplatte des Servers gespeichert. Die Files befinden sich anschließend z.B. im Verzeichnis `WTSRV / System32 / Clients / ICA` . Dort finden Sie eine weitere Verzeichnisstruktur vor, die die verschiedenen Clientversionen beinhaltet, z.B. `WFC16` für Windows 3.1x oder `WFC32` für Windows 95/98 und NT. Voraussetzung für die Installation des Clients über das Netzwerk ist ein Zugriff auf den MetaFrame Server mit einem der Protokolle IPX oder TCP/IP.

Setup

Um die Installation der Client-Software zu beginnen, wechseln Sie nun in das entsprechende Verzeichnis und bringen das Programm `SETUP.EXE` zur Ausführung. Anschließend erscheint das Begrüßungsfenster des Installationsprogramms. Hier wählen Sie den Button `Next` aus und gelangen zum nächsten Fenster, in dem Sie das Installationsverzeichnis angeben können. Das Programm erwartet die Angabe des `Program Folder`, gefolgt von der Angabe des Clientnamen. Wenn all diese Eingaben bestätigt wurden, beginnt die Installationsroutine mit dem Kopieren der Clientdateien. Die Installation ist hiermit beendet.

MetaFrame Client starten

Den MetaFrame Client starten Sie, indem über die Taskbar unter Programs/Citrix ICA Client das Programm `Remote Application Manager` ausgeführt wird. Wird der Client zum ersten Mal gestartet, erfolgt ein Hinweis, daß es noch keinen Eintrag für ein Connection Profile gibt. Bestätigen Sie mit `yes`, so kann direkt anschließend mit der Konfiguration des Profiles begonnen werden. Zuerst müssen Sie angeben, über welchen Typ die Verbindung zum MetaFrame Server aufgebaut werden soll. Zur Auswahl stehen die Optionen `NetWork`, `Dial-In` und `Serial`.

`NetWork`	Verbindung über das lokale Netzwerk wie auch remote über LAN-LAN-Kopplung via Router
`Dial-In`	Zugriff auf den Server via Modem
`Serial`	direkte Verbindung zwischen Client und Server mit Hilfe eines seriellen Kabels.

Tab.1: Verbindungen zum MetaFrame Server

Server

Das nächste Fenster fordert zur Eingabe eines Namens für das Connection-Profile und das zu verwendende Protokoll auf. In Abhängigkeit der zuvor gewählten Verbindungsart stehen z.B. für NetWork-Verbindungen die Protokolle IPX/NetBIOS/SPX und TCP/IP zur Verfügung. In unserem Fall verwenden wir eine Netzwerkverbindung über das TCP/IP-Protokoll. Als letzte Option in diesem Fenster wird eingestellt, ob eine Verbindung zum Server oder zu einer sogenannten `Published Application` aufgebaut werden soll. Der Begriff bedeutet, daß hier Applikationen im Netzwerk freigegeben und publiziert werden. Selektiert man z.B. `Server` und klickt mit der Maus auf den rechten nach unten weisenden Pfeil, so wird im LAN nach installierten WinFrame und MetaFrame

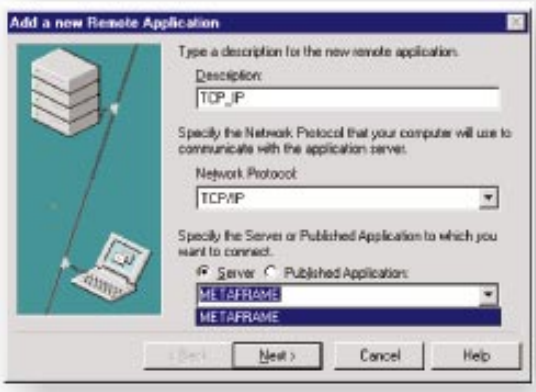


Abb. 1: Anlegen eines neuen Connection Profile

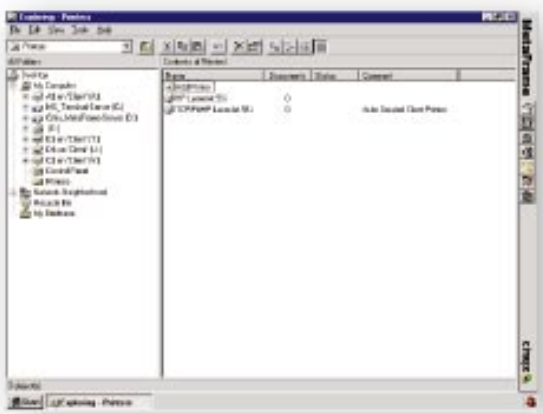


Abb. 2: Windows NT Explorer: verfügbare Ressourcen

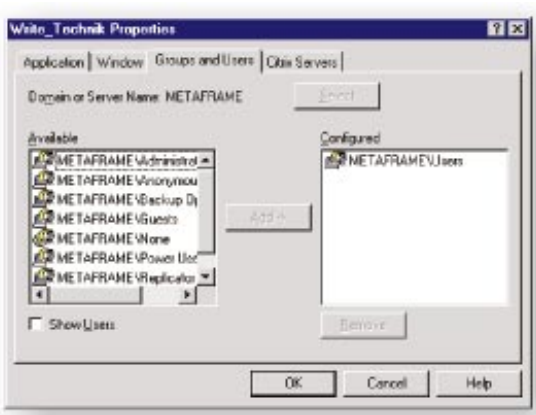


Abb. 3: Application Configuration: Auswahl von Gruppen oder Benutzern

Servern gesucht. Um die Server im Netzwerk bekannt zu geben, verwendet die MetaFrame Software einen mit Microsoft vergleichbaren Browsing-Dienst, der es ermöglicht, installierte WinFrame und Meta-Frame Server zu finden. Die Verbindung zum Server kann auch aufgebaut werden, wenn man an dieser Stelle dessen IP-Adresse konfiguriert, siehe Abb. 1.

Verbindungstyp

Im nächsten Menü wird angegeben, welcher Verbindungstyp zur Verfügung steht. Als Einstellungsmöglichkeiten sind angegeben:

- `I have a fast network connection` (LAN)
- `I have a low bandwith network connection` (WAN or Dial-Up NetWorking).

Da es sich in unserem Beispiel um eine LAN-Verbindung handelt, wählen wir an dieser Stelle die erste Option aus. Anschließend fragt die Setup-Routine nach `Username`, `Password` und `Domaine`. Diese Werte müssen an dieser Stelle nicht eingetragen werden. Wir erinnern uns, daß man diese Angaben ebenfalls mit Hilfe des Konfigurationsprogramms „Terminal Server Connection Configuration“ vornehmen kann. Sollten die Werte an dieser Stelle eingetragen und anschließend das Profile gestartet werden, so erfolgt eine automatische Anmeldung an den Server mit den betreffenden Daten.

Bildschirm

Der nächste Schritt des Setups führt uns zu einem weiteren Fenster, in dem man den Screen der Session an die lokale Bildschirmauflösung des Desktop anpassen kann. Je nachdem welche Auflösung gewählt wurde, erscheint das Session-Fenster in unterschiedlicher Größe. Anschließend kann noch spezifiziert werden, ob nach dem Einloggen am Server automatisch eine Applikation gestartet werden soll. Auch diese Einstellung haben wir bereits im Tool Terminal Server Connection Configuration gesehen. Doch an welcher Stelle nimmt man am besten die Einstellungen vor, am Client oder am Server? Wenn die Benutzer- oder Applikationseinstellungen am Client vorgenommen werden, so hat dies zur Folge, daß der jeweilige Anwender diese willkürlich ändern kann. Konfiguriert man diese Parameter hingegen am Server, so hat der Anwender keine Möglichkeit, die Einstellungen zu manipulieren.

Installation beenden

Im letzten Punkt des Installationsprogramm können Sie noch die Programmgruppe des Clients auswählen. Der abschließende Bildschirm bietet Ihnen die Möglichkeit, die Installation mit `Finish` zu beenden oder aber über `Back` die bisher durchgeführten Angaben zu ändern.

Verbindung zum MetaFrame Server

Die Verbindung zum MetaFrame Server wird durch einen Doppelklick mit der Maus auf das neu erstellte Connection Profile initiiert. Ein neu erscheinendes Fenster zeigt Ihnen den momentanen Verbindungsstatus an. Sollte die Connection zum Server nicht aufgebaut werden können, erscheint hier eine entsprechende Fehlermeldung, z.B. `Cannot connect to the Citrix Server, there is no route to the specified subnet address.`

Login

Wurde die Verbindung korrekt konfiguriert, erscheint in Abhängigkeit der Einstellungen des Clients entweder ein Anmeldefenster, wenn im Client kein Username und kein Password definiert wurde, oder aber das Einloggen wird automatisch durchgeführt,

weil Username und Password bereits eingetragen sind. Im ersten Fall müssen Sie also noch Eingaben vornehmen. Es handelt sich hierbei um einen normalen Windows NT User Account.
Nach erfolgtem Login am MetaFrame Server befinden Sie sich in der MetaFrame Session, die Ihnen einen Windows NT 4.0 Desktop zur Verfügung stellt. Abbildung 2 zeigt, welche Ressourcen im Windows NT Explorer zum Arbeiten bereitstehen, siehe Abb. 2.

In Tabelle 2 sehen wir die nutzbaren Laufwerke und Drucker, die sich wie folgt in Client- und Server-Ressourcen untergliedern. Sie können mit all den angegebenen Ressourcen arbeiten und zusätzlich alle auf dem MetaFrame- oder anderen Server installierten Applikation ausführen.

Applikationen eingrenzen

Es kann natürlich sein, daß der Administrator nicht möchte, daß die Clients mit Hilfe des NT-Explorers im Netzwerk nach installierten Applikationen suchen oder selbst ständig Drucker anlegen können. Oder aber es ist gewünscht, daß die Clients nur bestimmte Applikationen zur Verfügung gestellt bekommen. Im Laufe des Artikels haben wir gesehen, daß man den Start einer bestimmten Applikation an verschiedenen Stellen vorgeben kann.
Die Terminal Server Connection Configuration hat den Nachteil, daß pro selektiertem Protokoll nur eine Applikation zum automatischen Start genutzt werden kann. Der User Manager for Domains * hat ebenfalls den Nachteil, daß nur ein Programm pro User ausgewählt werden kann. Beim MetaFrame Client hingegen kann man mehrere Connection-Profiles mit dem gleichen Protokoll anlegen und pro Verbindung eine andere Applikation auswählen. Der Nachteil hierbei ist, daß je mehr Applikationen hinzukommen, es um so undurchsichtiger im Remote Applikation Manager wird. Außerdem sind die Anwender jetzt in der Lage, die Konfiguration beliebig zu ändern, was von Seiten des Administrators sicherlich nicht gewünscht wird.

Anm.: * Durch die Installation der Citrix MetaFrame Software wird bei den Eigenschaften der Benutzer ein neues Konfigurationsmenü mit dem Namen `Config` hinzugefügt, mit dessen Hilfe Einstellungen vorgenommen werden können, die ausschließlich für ICA Connections vorgesehen sind. Hierbei handelt es sich um eine Untermenge der Optionen, die mit dem Programm Terminal Server Connection Configuration zu definieren sind.

Application Publishing

Wegen der oben genannten Nachteile implementierte Citrix die Funktion des Application Publishing, um die Bereitstellung von Applikationen im Netzwerk wesentlich zu vereinfachen. Die Idee hierbei ist, den Citrix ICA Clients das Starten von Programmen zu ermöglichen, ohne daß der Client den Namen oder die Adresse des MetaFrame Server wissen muß. Um die Applikationen im Netzwerk zu publizieren, gibt es ein weiteres Utility, welches Sie über die Taskbar unter `Programs / MetaFrame Tools / Application Configuration` zur Ausführung bringen können. Eine neue „`Published Application`“ wird angelegt, indem Sie über die Menüleiste die Option `Application / New` auswählen. Zuerst wird nach einem logischen Namen für das Programm gefragt. Diesen sollten Sie so aussagekräftig wie möglich benennen. Über den Button `Next` gelangen Sie in ein weiteres Fenster, das Ihnen die Einstellungen `Explizit` und `Anonymous` bietet. Unter diesen Bezeichnungen verbergen sich die folgenden Funktionen:

Explizit oder anonym

Bei `Explizit` handelt es sich um einen gewöhnlichen MetaFrame User,

Laufwerke:	Client	Server	Typ
A$ on Client (A:)	x		Diskette
MS_Terminal-Server (C:)		x	Festplatte
Citrix_MetaFrame-Server (D:)		x	Festplatte
[E:]		x	CD-ROM
E$ on Client (T:)	x		Festplatte
D$ on Client (U:)	x		Festplatte
C$ on Client (V:)	x		Festplatte
Drucker:	**Client**	**Server**	**Typ**
HP Laserjet 5Si		x	Printer
TCPIP#HP Laserjet 5Si	x		Printer

Tab. 2: Client- und Server-Ressourcen

Abb. 4: ICA File Editor: Hinzufügen eines neuen Programms auf dem Windows Desktop

der für die Verbindung zum Server seine normalen Benutzerdaten benutzt, mit Username und Password. Ein Explizit User wird im User Manager for Domains angelegt.

Während der Installation von Citrix MetaFrame wurden bereits 15 `Anonymous User` – nämlich `Anon000` bis `Anon014` – und eine Gruppe namens `Anonymous` angelegt. Diese Benutzer besitzen die Rechte eines normalen Guest User unter Windows NT. Wenn nun eine Published Applikation mit Gastrechten ausgeführt werden kann, so ist ein Zugriff mit den Usern `Anonymous` ebenfalls möglich. Im Gegensatz zum `Explizit User` benötigt der `Anonymous User` keine Benutzerdaten, um sich im System anzumelden. Sie sollten diesem User nicht mehr Rechte als dem Guest Account geben, da man hierdurch eine Sicherheitslücke im Netzwerk schaffen würde. `Anonymous User` werden nur supported, wenn es sich bei dem Citrix MetaFrame Server nicht um einen Primary Domain Controller (PDC) oder Backup Domain Controller (BDC) handelt.

Applikationen freigeben

Für unsere Beispielkonfiguration verwenden wir den `Explizit User`. Im nächsten Konfigurations-Screen müssen wir den Pfad angeben, unter dem die Applikation gestartet werden kann. Um diese Eingaben zu vereinfachen, können mit Hilfe des Buttons `Browse` sowohl Server- als auch Netzwerklaufwerke durchsucht werden. Das folgende Menü gibt uns die Möglichkeit, die Titelleiste der Applikation zu unterdrücken und das Programm im maximierten Fenster zu starten. Anschließend wird definiert, welche User oder Gruppen Berechtigung zum Ausführen der Applikation erhalten sollen. Wenn Sie die Option `Show Users` aktivieren, können Sie einzelne User oder Gruppen selektieren, andernfalls nur Gruppen, siehe Abb. 3.

Das nächste Fenster gibt uns die Möglichkeit, den Server auszuwählen, auf dem die Applikation ausgeführt wird. Über die Option `Edit Configuration` können wir die bisher getätigten Einstellungen ändern, der Button `Next` führt uns zu einem weiteren Fenster, in dem die Installation der `Published Application` abgeschlossen wird. Anschließend befinden wir uns im Hauptbildschirm des Utility `Application Configuration`, wo nun das eben erstellte Programm zu sehen ist. Auf die gleiche Art und Weise lassen sich weitere Applikationen hinzufügen, die im Netzwerk verbreitet werden sollen.

Published Applications

Nachdem alle erforderlichen Applikationen angelegt wurden, kann der Administrator im Administrationsprogramm Terminal Server Connection Configuration für jedes Connection-Profil (protokollabhängig) bestimmen, ob es ab sofort nur noch möglich sein soll, `Published Applications` auszuführen. Dies geschieht unter `Eigenschaften / Connection Profile / Advanced – Option „Only run Published Application"`. Versucht nun ein Client eine Verbindung zum Server ohne `Published Application` aufzubauen, so wird dieser mit der Fehlermeldung `The system can not log you on (52E). Please try again or consult your system administrator` zurückgewiesen. Auf diese Art und Weise wird erzwungen, daß der Client nur noch eine Verbindung zum Server aufbauen kann, wenn anstatt des Servers eine Published Application konfiguriert wird. Loggt sich der Anwender anschließend im Server ein, wird das entsprechende Programm automatisch gestartet, beim Beenden der Applikation wird nicht nur diese, sondern die komplette Session terminiert.

ICA File Editor

Sie werden sich vielleicht fragen, wo der Vorteil einer Published Applikation gegenüber einer im Client oder Terminal Server Connection Configuration oder User Manager for Domains fest eingetragenen Applikation liegt.

Warum soll man Published Applications anlegen, wenn man doch auch mit diesen drei Utilities den Zugriff auf bestimmte Applikationen erzwingen kann. Der Grund liegt darin daß man Published Applications mit einem besonderen Programm mit dem Namen `ICA File Editor` bearbeiten und sehr komfortabel auf dem Desktop als Icon hinterlegen kann. Mit Hilfe dieses Utilities werden sogenannte ICA Files erstellt und verwaltet. Das sind Textdateien, die eine Reihe von Command Tags enthalten.

Diese Tags werden benutzt, um eine Applikation vom Server auszuführen, sie definieren bestimmte Attribute einer Session:

- Adresse des Citrix Server oder der Published Applikation
- Usernamen, Paßwort und Domäne, um sich am Server anzumelden
- Encryption Level für die Kommunikation mit dem MetaFrame Server
- Name der Applikations Definition

Wir wollen uns deshalb den ICA File Editor wegen seiner Vorzüge einmal genauer ansehen.

ICA File Editor installieren

Zuerst wollen wir die Installationsmöglichkeiten des ICA File Editor beschreiben. Zur Auswahl steht zunächst das Erstellen von Installationsdisketten über das Konfigurations-Tool `ICA Client Creator`, welches Sie in der Gruppe der MetaFrame Tools finden. Nachdem die Disketten kopiert wurden, können Sie den ICA File Editor am Client PC installieren. Zur Installation des ICA File Editor über eine bestehende LAN Verbindung finden Sie den Client auf dem Server im Verzeichnis `WTSRV \ SYSTEM32 \ CLIENTS \ ICA \ LCAEDIT \ DISKS \ Disk1`. Durch Ausführen der Datei `SETUP.EXE` wird die Installationsroutine gestartet, die uns als erstes fragt, ob der ICA File Editor installiert werden soll. Nach Bestätigung mit `yes` beginnt das Kopieren der entsprechenden Dateien auf die lokale Festplatte. Um die Möglichkeiten des Tools zu nutzen, ist an dieser Stelle ein Reboot der Workstation notwendig.

ICA File Editor starten

Der ICA File Editor wird gestartet, indem Sie in einem leeren Bereich auf Ihrem lokalen Desktop die rechte Maustaste betätigen und anschließend die Option `New/Citrix ICA Connection` selektieren. Daraufhin erscheint das erste Konfigurationsfenster, in dem alle vorher definierten Published Applications zur Auswahl stehen. Nach Angabe des zu verwendenden Programms gelangen wir zu einem weiteren Screen, wo der `Encryption Level` zur Kommunikation zwischen Client und Server anzugeben ist. Wir erinnern uns, daß dieser Level abhängig von den installierten Security-Produkten ist. Die nächste Option mit dem Namen `Compress Data Stream` ermöglicht es, den Datenstrom zu komprimieren. Dies ist besonders bei WAN-Verbindungen interessant, da hier meist nur eine geringe Bandbreite zur Verfügung steht. Zum Abschluß können Sie noch einen logischen Namen für die Remote Applikation eintragen und die Installation mit dem Button `Finish` beenden.

ICA Files bearbeiten

Anschließend befindet sich auf Ihrem lokalen Desktop ein neues Icon mit dem Citrix Logo, das den Namen des eben erstellten ICA File trägt. Als nächstes sollten Sie die Eigenschaften des Icons mit der rechten Maustaste selektieren und über die Registrierungskarte `Connection` den `Username` und das `Password` des Benutzers eingeben, unter dessen Account die Verbindung zum MetaFrame Server aufgebaut werden soll. Wenn nun ein Doppelklick auf das Icon ausgeführt wird, so startet automatisch eine Session, die sich mit den Benutzerdaten am Server anmeldet und zum Abschluß die Applikation startet, die im ICA File spezifiziert wurde. Wenn Sie dieses Verfahren nun für all Ihre notwendigen Applikationen durchführen, so ist das Anlegen von Connection Profiles im Remote Applikation Manager nicht mehr notwendig. Er wird gar nicht mehr benötigt.

Die Eigenschaften des vorher erstellten ICA File lassen sich nachträglich ändern, indem Sie die rechte Maustaste im ICA-Icon aktivieren. Hierauf hin erscheint ein Screen mit verschiedenen Einstellungsmöglichkeiten (vgl. Tab. 3.)

Der eigentliche Vorteil der ICA-Files besteht in der Integration der Remote-Applikationen in den lokalen Desktop. Jedes Programm, das durch diese ICA-File Session auf dem Citrix Server gestartet wurde, verhält sich genauso wie lokal ausgeführte Applikationen. Es besteht die Möglichkeit, die Remote-Applikation zu verkleinern oder zu vergrößern, d.h. sie wird in der Taskbar als Icon abgelegt oder von dieser wieder in den Vordergrund gestellt.

`General`	Es besteht die Möglichkeit, die Attribute des ICA- Files zu ändern. Defaultmäßig ist nur das Attribut Archive gesetzt.
`Security`	Die Zugriffsberechtigung auf das ICA-File kann für User und Gruppen nachträglich geändert werden.
`Address`	Option, sowohl den Citrix Server als auch die Published Applications zu wechseln.
`Connection`	Titel der Applikation und die Benutzer-Zugangsdaten lassen sich ändern
`Window`	Option, die Größe des Session-Fensters an die Auflösung des lokalen Desktop anzupassen.

Tab. 3: Einstellmöglichkeiten für ICA Files

Server Verwaltung

Zur Verwaltung des Citrix MetaFrame Server steht ein Utility zur Verfügung. Es läßt sich über die Taskbar unter `Programs / MetaFrame Tools / MetaFrame Administration` starten.

MetaFrame Administration

Das Eröffnungsfenster der MetaFrame Administration untergliedert sich in zwei Spalten. Auf der linken Seite finden Sie Informationen über die gefundenen Server, die angelegten Connection-Profiles mit den entsprechenden Protokollen, die Console – den User also, der sich direkt am MetaFrame Server angemeldet hat - und die momentan aktiven Sessions. Die rechte Seite stellt Informationen über Registrierkarten zur Verfügung, die sich in Abhängigkeit der links ausgewählten Option ändern (vgl. Tab. 4), siehe Abb. 5.

Session allokieren

Das Verwaltungstool MetaFrame Administration bietet noch eine Funktion, die dem Administrator des Citrix Server das Leben sehr vereinfacht. Wenn Sie bei einer aktiven Session die rechte Maustaste betätigen, so erscheinen die Eigenschaften dieser Sitzung. Einige Optionen wie z.B. Sende Message wurden bereits in obiger Übersicht erwähnt. Es gibt zudem noch die Option `Shadow`, die es ermöglicht, jede beliebige Session zu beobachten. Dies bedeutet, daß der Verwalter die Kontrolle über die Session erlangt. Dadurch wird es möglich, den entsprechenden Anwender bei Problemfällen zu unterstützen. Ob es dem Administrator erlaubt wird, eine Session zu allokieren, wird entweder anwenderbezogen über den

Linke Spalte	Registrierkarte	Bedeutung
All Listed Server	**Servers**	Auflisten aller Adressen, die dem Server zugewiesen wurde (abhängig von den installierten Protokollen, z.B. IP- & IPX-Adressen)
	Users	Anzeige der eingeloggten User und des Protokolls
	Sessions	Auflistung der momentan aktiven Sessions
	Processes	Liste der auf dem Citrix Server momentan aktiven Prozesse
	Licenses	Installierte Lizenzen und deren Status (Aktiviert, nicht frei geschaltet), User– und Poolcount, Lizenznummer.
Einzelner Server	**Users**	Anzeige der eingeloggten User und des Protokolls
	Sessions	Auflistung der momentan aktiven Sessions
	Processes	Liste der auf dem Citrix Server momentan aktiven Prozesse
	Licenses	Installierte Lizenzen und deren Status (Aktiviert, nicht frei geschaltet), User– und Poolcount, Lizenznummer.
	Information	Angabe der Software-Version des Terminal Server und der installierten Hotfixes.
Connection-Profiles		Mit Hilfe der rechten Maustaste können Sie alle Sessions, die zu dem entsprechenden Protokoll gehören, zurücksetzen.
Console	**Processes**	Auflistung der aktiven Console-Prozesse
Sessions	**Allgemein**	Mit Hilfe der rechten Maustaste sind Sie in der Lage, die Session zu disconnecten oder zurückzusetzen. Weiterhin besteht die Möglichkeit, dem User eine Nachricht zu übermitteln (Send Message)
	Processes	Zeigt an, welche Prozesse von der jeweiligen Session ausgeführt werden.
	Information	Angaben über die Client Software (Version, Installationsverzeichnis, Client Farbauflösung, Encryptionlevel ...)
	Modules	Auflistung aller vom Client ausgeführten Programme und DLLs
	Cache	Angaben über den Cache des Clients

Tab. 4: Informationen über Registrierkarten in Abhängigkeit der ausgewählten Option

User Manager for Domains oder protokollbezogen über das Programm Terminal Server Connection Configuration festgelegt. Tabelle 5 zeigt die Einstellungsmöglichkeiten. Die Funktion `Shadow` steht nur den Anwendern zur Verfügung, die den MetaFrame ICA Client auf ihren Workstations installiert haben. Bei Verwendung des Windows Terminal Server Client wird das Shadowing von Sessions nicht unterstützt. Weiterhin benötigt der User, der andere Sessions beobachten will, die Rechte als Mitglied der Gruppe Administrators. Man kann eine Session nur von einer separaten MetaFrame Client Workstation übernehmen, die Console des MetaFrame Server kann hierzu nicht benutzt werden (Abb. 6).

Eine herausragende Funktion der Citrix MetaFrame Software ist der Zugriff von Clients auf den Server über das Internet. Wie dieser Zugang realisiert wird, und was es hierbei zu beachten gilt, ist Gegenstand des nächsten Artikels unserer Citrix MetaFrame Serie.

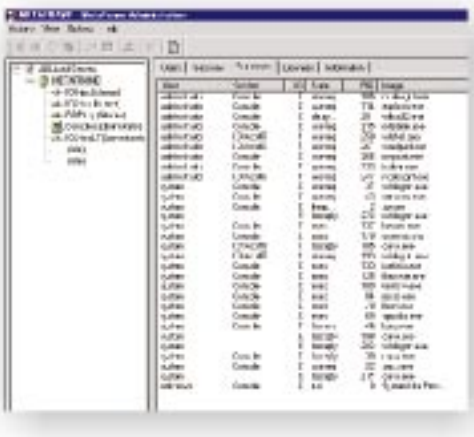


Abb. 5: MetaFrame Administration: Anzeige des Servers, Protokolle, Sessions, etc.

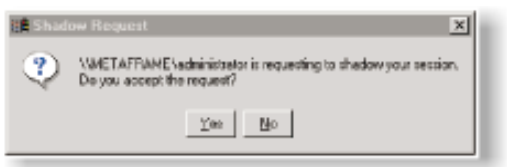


Abb. 6: Shadowing einer Benutzersession

Disabled	Shadowing wird nicht erlaubt
Enabled input On, notify On	Mit dieser Einstellung ist der Administrator in der Lage, Keyboard- und Mauseingaben in der allokierten Sitzung vorzunehmen (enabled input On). Der Parameter "notify On" bedeutet, daß der Anwender vor der Übernahme seiner Session durch den Administrator entsprechend informiert wird. An dieser Stelle hat der Benutzer die Möglichkeit, das Shadowing der Session zu erlauben oder abzuweisen.
Enabled input On, notify Off	Der Unterschied zur oben beschriebenen Option besteht im Parameter "notify Off". Diese Einstellungsmöglichkeit bedeutet, daß der User, dessen Session beobachtet werden soll, nicht informiert wird, wenn der Administrator die Kontrolle der Sitzung übernimmt.
Enabled input Off, notify On	Durch die Variable "input Off" ist es dem Administrator nicht möglich, Key- und Mauseingaben in der übernommenen Session, einzugeben.
Enabled input Off, notify Off	Wenn Sie diese Einstellung selektieren, so kann der Verwalter des Systems keine Keyboard- und Mauseingaben vornehmen, und der Benutzer wird vor der Übernahme der Session durch den Administrator nicht um Einverständnis gebeten.

Tab. 5: Einstellungsmöglichkeiten, Session zu allokieren, finden sich im User Manager for Domains oder in der Terminal Server Connection Configuration.

Problem erkannt, Gefahr gebannt

TCP/IP-Probleme unter Windows NT 4.0, Teil II

Wir haben uns im ersten Teil, in der TN 4/99, mit der Diagnose und Fehlerbehebung einiger häufig auftretender Kommunikationsprobleme unter Microsoft Windows NT beschäftigt, die bei der Verwendung von TCP/IP auftreten können. Im zweiten Teil gehen wir auf einzelne Dienste und bestimmte Vorgehensweisen zur Fehlerbehebung ein.

Die Anschlußeinstellungen für Dienste auf dem anderen Computer weichen möglicherweise von den Anschlußeinstellungen ab, die Sie zur Herstellung der Verbindung verwenden. In Tabelle 1 sind einige der Standardanschlußeinstellungen für verschiedene Protokolle aufgelistet.

Anschluß	Protokoll
80	HTTP
81	FTP
82	Telnet
70	Gopher

Tab. 1: Standardanschlüsse

Verwenden Sie das Dienstprogramm Telnet, um zu überprüfen, ob der andere Computer so konfiguriert wurde, daß Verbindungen über denselben Anschluß zulässig sind, den Sie zur Herstellung der Verbindung verwenden. Geben Sie hierzu an einer Eingabeaufforderung die folgende Zeile ein:

```
telnet <IP-Adresse> <Anschluß>
```

Dabei steht `<IP-Adresse>` für die IP-Adresse des anderen Computers und `<Anschluß>` für den Anschluß, über den Sie eine Verbindung herzustellen versuchen. Wird beispielsweise versucht, eine FTP-Verbindung zu dem anderen Computer über den Anschluß `21` herzustellen, geben Sie `telnet <IP-Adresse> 21` ein. Wird keine Fehlermeldung angezeigt, wurde der andere Computer so konfiguriert, daß Verbindungen über diesen Anschluß hergestellt werden können. Sie sollten daher in der Lage sein, unter Verwendung des entsprechenden Dienstes über diesen Anschluß eine Verbindung herzustellen. Wenn Sie eine Fehlermeldung erhalten, kann der andere Computer möglicherweise keine Verbindungen über diesen Anschluß herstellen. Stellen Sie sicher, daß Sie eine gültige Anschlußnummer für den Dienst auf dem anderen Computer zu erhalten.

Fehlgeschlagene Verbindung

Kann eine Verbindung zu dem anderen Computer unter Verwendung der IP-Adresse hergestellt werden, nicht aber unter Verwendung des Host- oder

NetBIOS-Namens, besteht möglicherweise ein Problem mit der Namensauswertung. Es können verschiedene Methoden angewendet werden, um die Namensauswertung in einem Netzwerk durchzuführen, z. B. die folgenden:
- HOSTS-Dateien
- DNS (Domain Name Service)
- LMHOSTS-Dateien
- WINS (Windows Internet Name Service)

Überprüfen Sie in jedem Fall diese Einstellungen, um zu erfahren, welche Methoden in Ihrem Netzwerk zur Namensauswertung verwendet werden. Führen Sie die in den folgenden Abschnitten beschriebenen Verfahren in der entsprechenden Reihenfolge durch. Überprüfen Sie nach jedem Verfahren, ob eine Verbindung zu dem anderen Computer unter Verwendung des Host- oder NetBIOS-Namens hergestellt werden kann.

HOSTS-Datei überprüfen

Bei der HOSTS-Datei handelt es sich um eine Textdatei, die mit einem beliebigen Texteditor bearbeitet werden kann. Wenn in Ihrem Netzwerk HOSTS-Dateien für die Hostnamensauswertung verwendet werden und Sie keine Verbindung zu dem anderen Computer unter Verwendung des Hostnamens herstellen können, liegt möglicherweise ein ungültiger Eintrag in der HOSTS-Datei vor. Suchen Sie in der HOSTS-Datei nach dem Hostnamen des anderen Computers, stellen Sie sicher, daß nur ein Eintrag pro Hostname vorhanden ist, und überprüfen Sie anschließend, ob der Eintrag für den Hostnamen des betreffenden Computers gültig ist. Weitere Informationen über die HOSTS-Datei finden Sie in der Beispieldatei `HOSTS` im Ordner `%System Root%\System32\Drivers\Etc`.

DNS-Konfiguration überprüfen

Die Hostnamensauswertung kann mit Hilfe eines Domain Name Service Servers durchgeführt werden. Wenn in Ihrem Netzwerk DNS zur Hostnamensauswertung verwendet wird und Sie keine Verbindung zu dem anderen Computer unter Verwendung des Hostnamens herstellen können, besteht möglicherweise ein Problem mit der DNS-Konfiguration Ihres Computers oder mit dem DNS-Server in Ihrem Netzwerk. Um festzustellen, ob das Problem durch die DNS-Konfiguration Ihres Computers verursacht wird, führen Sie folgende Schritte durch:

1. Geben Sie an einer Eingabeaufforderung `ipconfig /all` ein, um die IP-Adresse des DNS-Servers anzuzeigen. Wird die IP-Adresse für den DNS-Server nicht angezeigt, wenden Sie sich an Ihren Netzwerkadministrator, um die IP-Adresse für den DNS-Server zu erhalten.

2. Stellen Sie sicher, daß Sie eine Verbindung zum DNS-Server herstellen können, indem Sie Ping für die IP-Adresse des DNS-Servers ausführen. Es sollten Informationen wie die folgenden angezeigt werden:

```
PING wird ausgeführt für <###.###.###.###> mit 32 Bytes Daten:
Antwort von <###.###.###.###>:  Bytes=32 Zeit=77ms TTL=28
Antwort von <###.###.###.###>:  Bytes=32 Zeit=80ms TTL=28
```

Dabei steht `<###.###.###.###>` für die IP-Adresse des DNS-Servers.

Ping schlägt fehl

Schlägt die Ausführung von Ping für die IP-Adresse des DNS-Servers fehl, versuchen Sie sicherzustellen, daß Sie die richtige IP-Adresse für den DNS-Server verwenden. Sie sollten überprüfen, ob der DNS-Server mit dem Netzwerk verbunden ist und einwandfrei funktioniert. Wenn Sie Ping für die IP-Adresse des DNS-Servers ausführen können, die Hostnamensauswertung für den anderen Computer jedoch nicht möglich ist, wertet der DNS-Server die Hostnamen möglicherweise nicht korrekt aus. Stehen mehrere DNS-Server in Ihrem Netzwerk zur Verfügung, konfigurieren Sie Ihren Computer für die Verwendung eines anderen DNS-Servers. Wenn der Hostname des betreffenden Computers auf einem anderen DNS-Server korrekt ausgewertet werden kann oder kein anderer DNS-Server zur Verfügung steht, versuchen Sie das Problem auf dem ursprünglichen DNS-Server zu beheben. Nachdem Sie sichergestellt haben, daß die korrekte IP-Adresse für den DNS-Server verwendet wird, aktualisieren Sie die TCP/IP-Einstellungen Ihres Computers. Wenn Sie sich über eine DFÜ-Verbindung mit dem Netzwerk verbinden, müssen Sie lediglich die TCP/IP-Einstellungen im Telefonbucheintrag des DFÜ-Netzwerks ändern, so daß dieser die korrekte IP-Adresse für den DNS-Server enthält.

Gültige IP-Adresse

Um eine gültige IP-Adresse für den DNS-Server in den TCP/IP-Einstellungen Ihres Computers hinzuzufügen oder zu ändern, führen Sie folgende Schritte durch:

1. Doppelklicken Sie in der Systemsteuerung auf `Netzwerk`, und klikken Sie anschließend auf die Registerkarte `Protokolle`.

2. Wählen Sie das `TCP/IP` Protokoll aus, indem Sie darauf klicken, klikken Sie auf `Eigenschaften` und anschließend auf die Registerkarte `DNS`.

3. Wird ein DNS-Server hinzugefügt, klicken Sie auf `Hinzufügen`. Soll ein vorhandener Server bearbeitet werden, klicken Sie auf die `IP-Adresse` für den entsprechenden DNS-Server, und klicken Sie anschließend auf `Bearbeiten`.

4. Geben Sie die korrekte IP-Adresse für den DNS-Server ein, und klicken Sie anschließend auf `OK`.

5. Klicken Sie auf `OK` und anschließend nochmals auf `OK`.

Es ist zu empfehlen, den Rechner im Anschluß an diesen Schritt neu zu starten.

TCP/IP im DFÜ-Netzwerk

Um eine gültige IP-Adresse für den DNS-Server in einem Telefonbucheintrag des DFÜ-Netzwerks hinzuzufügen oder zu ändern, führen Sie folgende Schritte durch:

1. Klicken Sie im DFÜ-Netzwerk auf den entsprechenden Eintrag im Feld `Telefonbucheintrag`.
2. Klicken Sie auf `Weiteres`, und klicken Sie anschließend auf `Eintrags- und Modemeigenschaften bearbeiten`.
3. Klicken Sie auf die Registerkarte `Server`, anschließend auf die Schaltfläche `TCP/IP-Einstellungen`.
4. Klicken Sie auf `Namens-Server-Adressen angeben` und geben Sie anschließend die korrekte IP-Adresse im Feld `Primärer DNS` ein.

LMHOSTS-Datei überprüfen

Bei der LMHOSTS-Datei handelt es sich um eine Textdatei, die mit einem beliebigen Texteditor bearbeitet werden kann. Wenn in Ihrem Netzwerk LMHOSTS-Dateien für die NetBIOS-Namensauswertung verwendet werden und Sie keine Verbindung zu dem anderen Computer unter Verwendung des NetBIOS-Namens herstellen können, liegt möglicherweise ein ungültiger Eintrag in der LMHOSTS-Datei vor. Suchen Sie in der LMHOSTS-Datei nach dem NetBIOS-Namen des anderen Computers, stellen Sie sicher, daß nur ein Eintrag pro NetBIOS-Name vorhanden ist, und überprüfen Sie anschließend, ob der Eintrag für den NetBIOS-Namen des betreffenden Computers korrekt ist. Sind Einträge mit `#INCLUDE` oder Zeilenblöcke mit `#BEGIN_ALTERNATE` und `#END_ALTERNATE` in der LMHOSTS-Datei enthalten, deaktivieren Sie diese Zeilen oder Zeilenblöcke vorübergehend, indem Sie am Anfang jeder Zeile, die deaktiviert werden soll, ein Nummernzeichen (#) und ein Leerzeichen eingeben. Wird das Problem durch das Deaktivieren dieser Zeilen oder Zeilenblöcke gelöst, reaktivieren Sie nacheinander die Zeilen oder Zeilenblöcke, bis das Problem erneut auftritt. Falls Sie feststellen, daß eine bestimmte Zeile oder ein bestimmter Zeilenblock ein Problem verursacht, überprüfen Sie die LMHOSTS-Datei, auf die die Zeile oder der Zeilenblock verweist. Weitere Informationen über die LMHOSTS-Datei finden Sie in der Beispieldatei `Lmhosts.sam`, die sich im Ordner `%SystemRoot%\System32\Drivers\Etc` befindet.

WINS überprüfen

Die NetBIOS-Namensauswertung kann mit Hilfe eines WINS-Servers (Windows Internet Name Service) durchgeführt werden. Wenn in Ihrem Netzwerk WINS zur NetBIOS-Namensauswertung verwendet wird und Sie keine Verbindung zu dem anderen Computer unter Verwendung des NetBIOS-Namens herstellen können, besteht möglicherweise ein Problem mit der WINS-Konfiguration Ihres Computers oder mit dem WINS-Server in Ihrem Netzwerk. Um festzustellen, ob das Problem durch die WINS-Konfiguration Ihres Computers verursacht wird, führen Sie folgende Schritte durch:
1. Geben Sie an einer Eingabeaufforderung `ipconfig /all` ein, um die IP-Adresse des WINS-Servers anzuzeigen. Wird die IP-Adresse für den WINS-Server nicht angezeigt, versuchen Sie die IP-Adresse für den WINS-Server zu erhalten.
2. Stellen Sie sicher, daß Sie eine Verbindung zum WINS-Server herstellen können, indem Sie Ping für die IP-Adresse des WINS-Servers ausführen. Es sollten Informationen wie die folgenden angezeigt werden:

```
PING wird ausgeführt für <###.###.###.###> mit 32 Bytes Daten:
Antwort von <###.###.###.###>:  Bytes=32 Zeit=77ms TTL=28
Antwort von <###.###.###.###>:  Bytes=32 Zeit=80ms TTL=28
Antwort von <###.###.###.###>:  Bytes=32 Zeit=78ms TTL=28
```

Dabei steht `<###.###.###.###>` für die IP-Adresse des WINS-Servers.

Kein Ping auf WINS-Server

Kann Ping für die IP-Adresse des WINS-Servers nicht ausgeführt werden, versuchen Sie sicherzustellen, daß Sie die richtige IP-Adresse für den WINS-Server verwenden. Überprüfen Sie, ob der WINS-Server mit dem Netzwerk verbunden ist und einwandfrei funktioniert. Wenn Sie Ping für die IP-Adresse des WINS-Servers ausführen können, die NetBIOS-Namensauswertung für den anderen Computer jedoch nicht möglich ist, wertet der WINS-Server die NetBIOS-Namen möglicherweise nicht korrekt aus. Stehen mehrere WINS-Server in Ihrem Netzwerk zur Verfügung, konfigurieren Sie Ihren Computer für die Verwendung eines anderen WINS-Servers. Wenn der NetBIOS-Name des betreffenden Computers auf einem anderen WINS-Server korrekt ausgewertet werden kann oder kein anderer WINS-Server zur Verfügung steht, bitten Sie Ihren Netzwerkadministrator, das Problem auf dem ursprünglichen WINS-Server zu beheben. Nachdem Sie sichergestellt haben, daß die korrekte IP-Adresse für den WINS-Server verwendet wird, aktualisieren Sie die TCP/IP-Einstellungen Ihres Computers.

DFÜ-Verbindung zum Netzwerk

Wenn Sie sich über eine DFÜ-Verbindung mit dem Netzwerk verbinden, müssen Sie lediglich die TCP/IP-Einstellungen im Telefonbucheintrag des DFÜ-Netzwerks ändern, so daß dieser die korrekte IP-Adresse für den WINS-Server enthält. Um eine gültige IP-Adresse für den WINS-Server in den TCP/IP-Einstellungen Ihres Computers hinzuzufügen oder zu ändern, führen Sie folgende Schritte durch:
1. Doppelklicken Sie in der Systemsteuerung auf `Netzwerk`, und klikken Sie anschließend auf die Registerkarte `Protokolle`.
2. Wählen Sie das TCP/IP-Protokoll aus, indem Sie darauf klicken, klikken Sie auf `Eigenschaften` und anschließend auf die Registerkarte `WINS-Adresse`.
3. Geben Sie im Feld `Primärer WINS-Server` die korrekte IP-Adresse für den WINS-Server ein, und klicken Sie anschließend auf `OK`.
4. Klicken Sie auf `Schließen`, anschließend auf `Ja`, um den Computer neu zu starten.

Jahr-2000-fähig ?

Backup-Produkte fürs neue Jahrtausend

Häufig wird an uns schon die Frage gerichtet, welche Backup-Produkte von Cheyenne bzw. Computer Associates Jahr-2000-fähig sind. Die nachfolgende Liste gibt Auskunft.

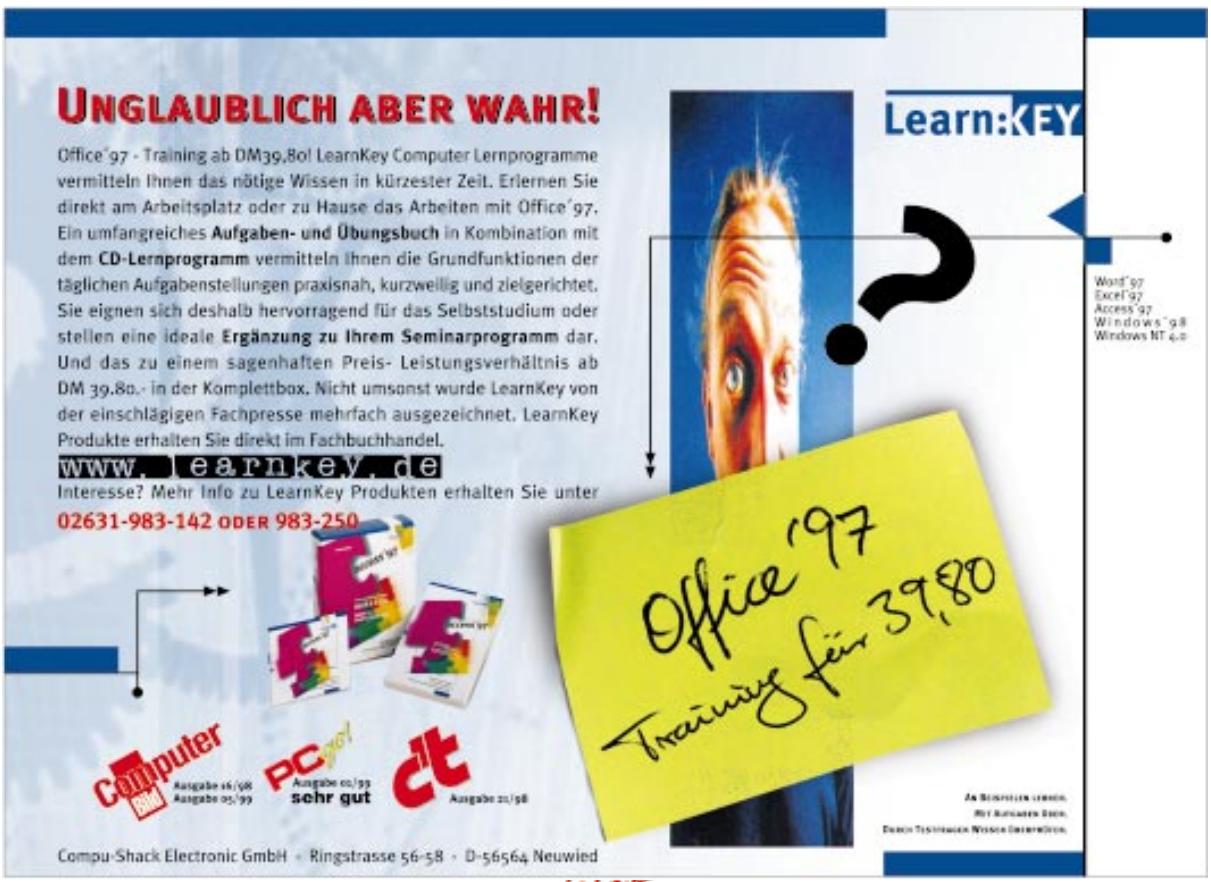
Jahr-2000-fähig

ARCserve für Intranetware für Small Business 6.1 (SP2)
ARCserve für NetWare, 10 User Edition 6.1 (SP2)
ARCserve für NetWare, Enterprise Edition 6.1 (SP2)
ARCserve für NerWare, Single Server Edition 6.1 (SP2)
ARCserve für NetWare, Workgoup Edition 6.1 (SP2)
ARCserve für Windows NT - Enterprise Edition 6.0 und höher
ARCserve für Windows NT - Single Server Edition 6.0 und höher
ARCserve für Windows NT - Workstation Edition 6.0 und höher
ARCserveIT Agent für MS Exchange 6.6
ARCserveIT für NetWare 6.6
ARCserveIT für NT 6.6
Changer (Autoloader) Option 3.1
Changer Option für Arcserve für Windows NT 2.0
Cheyenne Disaster Recovery 1.0 und höher
Client Agent für Windows 1.0 und höher
Client Agent für Windows 95 3.0
Client Agent für Windows NT 1.02 ; 3.0; 4.0
Client Push Agent für NetWare 2.1

Nicht Jahr-2000-fähig

Nachfolgend sind die Backup-Produkte aufgeführt, welche nicht Jahr-2000-fähig sind:
ARCserve 4.x für NetWare
ARCserve 5.x für NetWare
ARCSOLO für DOS
ARCSOLO für OS/2 Professional
ARCSOLO für Windows
ARCSOLO für Windows 95

Eine Gesamtaufstellung aller CA- Produkte finden Sie unter: `http: // www.cai.com /products / ca2000 /Y2Kready_list.htm`


UNGLAUBLICH ABER WAHR!
Office'97 - Training ab DM39,80! LearnKey Computer Lernprogramme vermitteln Ihnen das nötige Wissen in kürzester Zeit. Erlernen Sie direkt am Arbeitsplatz oder zu Hause das Arbeiten mit Office'97. Ein umfangreiches Aufgaben- und Übungsbuch in Kombination mit dem CD-Lernprogramm vermitteln Ihnen die Grundfunktionen der täglichen Aufgabenstellungen praxisnah, kurzweilig und zielgerichtet. Sie eignen sich deshalb hervorragend für das Selbststudium oder stellen eine ideale Ergänzung zu Ihrem Seminarprogramm dar. Und das zu einem sagenhaften Preis- Leistungsverhältnis ab DM 39.80,- in der Komplettbox. Nicht umsonst wurde LearnKey von der einschlägigen Fachpresse mehrfach ausgezeichnet. LearnKey Produkte erhalten Sie direkt im Fachbuchhandel.
www.learnkey.de
Interesse? Mehr Info zu LearnKey Produkten erhalten Sie unter
02631-983-142 ODER 983-250
Learn:KEY
Word'97
Excel'97
Access'97
Windows'98
Windows NT 4.0
Office '97
Training für 39,80
sehr gut
Compu-Shack Electronic GmbH · Ringstrasse 56-58 · D-56564 Neuwied

Gesagt, getan

Tips der Hotline, Teil 1

Wofür ist die Datei ARCHIVE.REF eigentlich da? Welche Dateien müssen gelöscht werden, um den David- oder FaxWare-Client neu zu installieren? Und was bedeutet die Windows NT Fehlermeldung 2186? Wir haben einige interessante Lösungen und Tips aus der Tobit-Hotline für Sie zusammengetragen.

Wenn Sie auf einem NetWare Server einmal ein PURGE durchgeführt haben, werden Sie sich sicherlich gefragt haben, woher die unzähligen Dateien mit dem Namen ARCHIVE.REF stammen. Diese Dateien werden im Zuge der nächtlichen Datenbereinigung in jedem Archiv angelegt. Der erste Teil der Bereinigung prüft alle Dateien in Ihren Archiven und schreibt alle Dateien, die referenziert werden konnten, in die Datei ARCHIVE.REF. Im nächsten Durchlauf der Bereinigung wird geprüft, ob die zu löschende Datei in der ARCHIVE.REF aufgetaucht ist. Ist dies nicht der Fall, so wird diese Datei für den nächsten Schritt der Bereinigung, dem Löschen markiert. Im letzten Schritt werden nun alle Dateien in den Archiven gelöscht, welche nicht in der ARCHIVE.REF aufgeführt sind. Anschließend wird die ARCHIVE.REF aus dem Archiv gelöscht.

Platz für Client

Falls es nach dem Einspielen eines Service Packs für David 5.xx oder FaxWare 5 zu Problemen kommt, sollten Sie in jedem Fall auch den Client neu installieren, damit Sie die aktuellen Dateien aus dem David-Verzeichnis auch auf Ihrem Client haben. Sollte nach einer solchen Installation der Client nicht ordnungsgemäß arbeiten, so kann dieses an einem Datei-Mischmasch liegen. Um dieses Problem zu beseitigen, sollten Sie den Client neu installieren, doch zuvor die alten David-Dateien von Ihrem Client löschen. Für eine Neuinstallation der Client Software löschen Sie bitte folgende Dateien aus dem Windows Root-Verzeichnis:

DVWIN.EXE
DVWIN$.GER
DVWIN$.ENG
DVWIN$.FRA
DVEDIT.EXE
DVEDIT$.GER
DVEDIT$.ENG
DVEDIT$.FRA
DVAPI.DLL
DVWIN$.AUX
DVEDIT$.AUX
FAXWARE.DRV
FAPI.DLL
UNIDRV.DLL
TOBITLIB.DLL
TOBIT.INI

Dateien löschen

Achten Sie darauf, daß sich keine dieser Dateien mehr in einem Windows Unterverzeichnis befindet. Sollten Sie vorher einmal ein FaxWare Frontend installiert haben, so löschen Sie bitte auch alle Dateien FW*.* im Windows Verzeichnis. Entfernen Sie ebenfalls den Druckertreiber FaxWare bzw. Tobit FaxWare aus der Druckerkonfiguration und löschen Sie bitte aus der SYSTEM.INI bzw. WIN.INI evtl. vorhandene Einträge von David. Wenn sich einzelne Dateien nicht löschen lassen, kann das daran liegen, daß diese in den Windows-Speicher geladen wurden. Mit dem Tool MODULES, das Sie auf dem Server im Verzeichnis DAVID\UTIL\WINDOWS finden, lassen sich diese Dateien entladen. Nach einem Neustart des Rechners starten Sie das SETUP.EXE Programm für den David Client erneut aus dem Verzeichnis DAVID\CLIENTS.

Ein- und Ausgangsbücher

In der Tobit FaxWare hatten Sie die Möglichkeit, sich das globale Sende- und Empfangsbuch anzusehen. Dazu mußten Sie lediglich für den

jeweiligen Benutzer den Schalter Einträge aller Benutzer im Service-Layer auf JA setzen. Dieser Schalter steht Ihnen in David nicht mehr zur Verfügung. Allerdings können Sie sich auch hier noch die globalen Sende- und Empfangsbücher ansehen. Dazu sollten Sie zuerst festlegen, in welchem Archiv Sie die globalen Protokolle angezeigt bekommen möchten. Mit Hilfe der DupLog-Funktion wird eine Kopie vom Sende- und Empfangsprotokoll erstellt. Hierfür müssen zwei Einträge in der DAVID.INI vorgenommen werden (vgl. Tab. 1). Den genauen Pfad können Sie am David Client über die Archive-Eigenschaften abfragen. Die DupLog-Parameter werden in geschweiften Klammern angeben (vgl. Tab. 2).

DupLog-Einträge

Mittels der DupLog-Einträge in der DAVID.INI werden in das Ein- und Ausgangsarchiv der Gruppe die globalen Empfangs- und Sendeprotokolle, die Dateien DAVID.LOG und DAVID.REC geführt. Der Inhalt dieser beiden Dateien wird in die Datei ARCHIVE.DAT geschrieben. Diese Datei ermöglicht Ihnen die Anzeige der Protokolle in dem Ein- und Ausgangsbuch der Gruppe. Bei den globalen Protokollen gibt es allerdings eine Kleinigkeit zu beachten. Die Einträge in diesen Protokollen sind ja nur „Verknüpfungen“ zu den jeweiligen Einträgen in den Archiven. Wenn nun Einträge in den Archiven manuell oder per automatischer Datenbereinigung gelöscht werden, so werden die eigentlichen Images, die Faxe, E-Mails und Attachments, erst dann von der Platte gelöscht, wenn auch die entsprechenden Verknüpfungen, also die Einträge in den globalen Protokollen, gelöscht werden. Wenn dieses nicht beachtet wird, kann das u.U. zu sehr großen Datenmengen führen.

Service-Layer

Wenn Sie unter NetWare über den Hotkey [ALT+I] im DAVID.NLM die DAVID.INI editieren, so brauchen Sie den Service-Layer nicht erneut zu starten. Falls Sie auf andere Weise als unter Windows NT die DAVID.INI editieren, so sollten Sie den Service-Layer wohl erneut starten. Anmerkung: Die Globalen Protokolle dienen nur der Anzeige. Das Einrichten einer Verteilung für ein solches globales Protokoll ist nicht möglich. Ein Verschieben von Nachrichten aus einem globalen Protokoll sollte nach Möglichkeit vermieden werden, da die originale Nachricht aus dem Archiv des Users verschwindet. Wird aus diesem globalen Protokoll nun ein Eintrag von einem User abermals versendet oder verteilt, so erscheint dieser nicht erneut im globalen Protokoll, sondern in seinem persönlichen Protokoll.

NT Fehlermeldung 2186

Wenn der Service-Layer unter Windows NT zwar noch über die Auswahlmaske unter Dienste angewählt und beendet werden kann, aber anschließend der Dienst auf keine Kontrollfunktionen reagiert und als gestartet oder bereits beendet gemeldet wird, kontrollieren Sie erst einmal im Taskmanager über [STRG + ALT+ ENTF], ob die SL.EXE dort noch als Task geführt wird. Hierüber sollten Sie dann versuchen, diesen Task zu beenden.

Ist dieses nicht der Fall, können Sie über die Eingabeaufforderung versuchen, den Dienst über den Befehl NET START DAVID SERVICE-LAYER oder NET STOP DAVID-SERVICELAYER manuell zu starten bzw. zu entladen. Ist dieses ebenfalls nicht möglich, muß der Server neu gestartet werden. Hierbei ist zu beachten, daß möglicherweise ein fehlerhafter Auftrag den Service-Layer als Task inaktiv geschaltet hat.

Tab. 1: DupLog Einträge in der DAVID.INI

NetWare

```
DupLog={RX}SYS:DAVID\ARCHIVE\GROUP\»Group-ID«\IN\ARCHIVE.DAT
DupLog={TX}SYS:DAVID\ARCHIVE\GROUP\»Group-ID«\OUT\ARCHIVE.DAT
Windows NT
DupLog={RX}\\SERVERNAME\DAVID\ARCHIVE\GROUP\»Group-ID«\IN\ARCHIVE.DAT
DupLog={TX}\\SERVERNAME\DAVID\ARCHIVE\GROUP\»Group-ID«\OUT\ARCHIVE.DAT
```

Tab.2: DupLog-Parameter

RX	nur Empfangsbucheinträge
TX	nur Sendebucheinträge
–	nur fehlerhafte Einträge
!	nur Einträge mit Abschlußstatus DOCTYPE=n, wobei n einen der folgenden Werte haben kann:
0	nur Fax
1	Directory (nicht verwendbar für das DupLog)
2	nur Mail
3	nur TMail
4	nur Voice

Reboot

Da der Dienst in der Diensteliste standardmäßig auf die Startoption AUTOMATISCH gesetzt ist, würde die Ursache den Fehler gleich wieder hervorrufen. Sie sollten die Startoption des Service-Layer-Dienstes folglich auf MANUELL setzen und den Server rebooten. Nach dem Start des Servers ist zu kontrollieren, ob ein beschädigter Auftrag vorliegt. Hierzu sollten Sie zunächst im Verzeichnis DAVID\APPS\FAXWARE\OUT\API kontrollieren, ob dort eine Datei ohne Extension vorliegt. Löschen Sie diese gegebenenfalls und auch die DAVID.JOB im Verzeichnis DAVID\CODE. Wenn es ein Beschädigung beim Empfang/Versand gab, finden Sie das entsprechende RX/TX File im Verzeichnis DAVID\TLD\PORT\00X. Anschließend sollten die Dienste korrekt gestartet werden können. Der Effekt ist gegebenenfalls durch einen beschädigten Auftrag entstanden. Dies kann unter Umständen über die Delay-Parameter in der DAVID.INI im Verzeichnis DAVID\CODE behoben werden. Setzen Sie diese dann einmal auf einen höheren Wert. Beachten Sie, daß die Parameter erst nach einem Neustart der Dienste ausgewertet werden.

E-Mail an Faxnummer

In David / FaxWare haben Sie die Möglichkeit, empfangene Faxe über einen Eintrag im Service-Layer bzw. DVAdmin an eine andere Faxnummer weiterzuleiten.
Diese Einstellungen nehmen Sie in dem Menüpunkt EMPFANG/WEITERSENDEN AN in der Benutzerkonfiguration vor.
Auf diesem Wege können Sie nun aber auch empfangene E-Mails an eine bestimmte Faxnummer weiterleiten. Dazu nutzen Sie den FileScan Service von David bzw. FaxWare.

FileScan Service

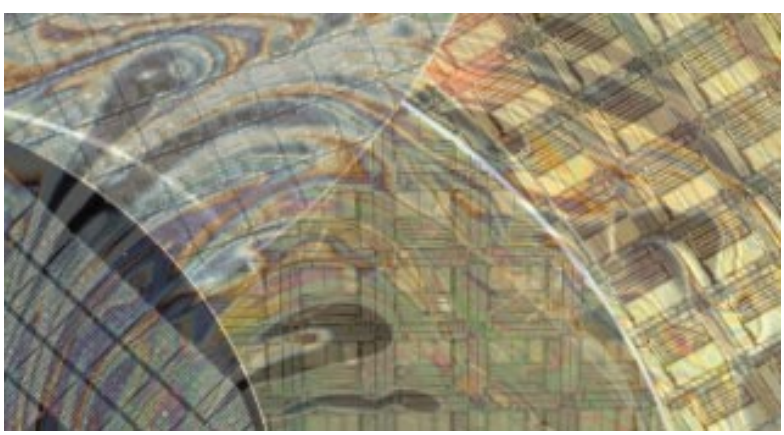
Um den FileScan Service zu konfigurieren, erstellen Sie zuerst im David Client ein Archiv - z.B. eMail_to_Fax - in das alle E-Mails, welche an die Faxnummer weitergeleitet werden sollen, als Kopie verteilt werden. Über die Archive-Eigenschaften haben Sie nun die Möglichkeit, in der Kartei PFAD-INFO den Pfad zu diesem Archiv zu markieren und auszuschneiden.
Wechseln Sie in den Service-Layer bzw. den DVAdmin und wählen Sie den Menüpunkt KONFIGURATION/SERVICES/FILESCAN SERVICE. Durch Betätigen der Einfügetaste können Sie einen neuen Eintrag für diesen Service generieren.
Als Pfad fügen Sie den soeben im Client kopierten Pfad zu dem Group-Archive ein. Ergänzen Sie die Pfadangabe durch die Angabe *.001. In diesem Fall sähe eine Pfadangabe wie folgt aus: \\Servername \DAVID \ARCHIVE \GROUP \Verzeichnisname *.001. Als Datenformat wählen Sie entweder STANDARD oder PCL FAX. Bei Verwendung des Formates PCL FAX muß allerdings der PCL Conversion Server gestartet sein.
Unter Windows NT wird dieser als Dienst, unter Novell NetWare als NLM durch Eingabe von PCL an der Serverkonsole geladen.
Menüpunkt INCLUDE DATEI die soeben erstellte Datei als Abschluß-Include-Datei an. Speichern Sie diese Einstellung.
Wenn nun an dieses Archiv eine Mail verteilt wird, so wird diese Nachricht in das Faxformat gewandelt und an die in der INCLUDE Datei angegebenen Faxnummer gesendet.

ICP VORTEX

Tips und Trick für GDT

ICP Controller der GDT RP Serie auch ohne CPU-Kühler

Für die Fertigung der ICP Controller der GDT RP-Serie kommen u.a. auch die Intel i960RP® Prozessoren zum Einsatz. Dieser Chip ist in zwei Versionen verfügbar, wobei beide Versionen funktional und leistungsmäßig identisch sind. Der einzige Unterschied ist die Versorgungsspannung: 5 Volt oder 3.3 Volt. Beim Einsatz der 3.3 Volt Type entsteht eine geringere Verlustleistung, so daß der CPU-Kühler des GDT RP-Serie Controllers nicht mehr benötigt wird. Sollte Ihr RP-Serie Controller also über keinen CPU- Kühler verfügen, ist dies beabsichtigt.



SIMMs

Der Speichercontroller der GDT RP-Serie ist sehr flexibel und kann sowohl Fast Page Mode (FPM) SIMMs, als auch Extended Data Out (EDO) SIMMs ansteuern. Die Organisation des SIMMs kann entweder 32 Bit (keine Parity), oder 36 Bit (Parity) sein. Der GDT RP-Serie Controller erkennt automatisch die Größe des SIMMs (4MB, 8MB, 16MB, 32MB oder 64MB) und die Organisation. Da eine einfache und eindeutige automatische Erkennung von FPM oder EDO SIMMs nicht möglich ist, wird auf den GDT RP-Serie Controller per Jumper eingestellt, ob es sich um einen FPM oder einen EDO SIMM handelt. Ein geschlossener Jumper „S1“ bedeutet, daß der Speichercontroller davon ausgeht, daß es sich bei dem installierten SIMM um ein EDO SIMM handelt. Bleibt „S1“ offen, wird der eingesteckte SIMM im Fast Page Mode betrieben. Die Leistung des GDT Controllers wird mit einem EDO SIMM erheblich gesteigert.

50 ns und 60 ns

Aufgrund des Designs des i960RP® Prozessors müssen die eingesetzten SIMMs bei EDO 50 ns und FPM 60 ns Zykluszeit erlauben. 50 ns EDO SIMMs werden von der Fa. Micron Technology (USA) hergestellt und können u.a. über die Distribution bezogen werden. In den ICP-Testlabors wurden außerdem sehr viele unterschiedliche 60 ns EDO SIMMs erfolgreich qualifiziert. Da in der Regel die Hersteller der DRAM-Bausteine nicht zugleich die SIMMs herstellen, ist eine Lieferantenangabe hier schwierig. Problematisch kann es bei SIMMs werden, die aus vielen einzelnen DRAMs zusammengesetzt sind. Wenn Sie den Speichertest in GDT SETUP auf „intensiv“ stellen und das Komplettsystem einem gründlichen Testlauf unterziehen, sind auch 60 ns EDO SIMMs erfolgreich verwendbar. Sollte ein vermeintlicher 60 ns EDO SIMM doch einmal nicht richtig funktionieren, können Sie durch Öffnen des „S1“ Jumpers in den FPM-Betrieb umschalten. Dann sollte auch dieser SIMM problemfrei arbeiten.

NOVELL

NetWare IP

Service-spezifische IP-Portnummern

Jeder kennt das Problem der IP-Filter. Egal ob Sie Kosten sparen möchten oder aus Sicherheitsgründen, um einen Filter zu definieren, der nicht auf Mac-Ebene ansetzt, sondern sich an bestimmte Services oder Programme richtet, müssen Sie die entsprechende Portnummer kennen, die von den einzelnen Services verwendet werden.

Fest zugeteilte Portnummern kann man in der RFC 1700 nachlesen. Hierunter sind die Ports von 1 bis 1023 definiert. Alle anderen Ports oberhalb dieser Grenze sind für Zusatzfunktionen gedacht und werden von den Herstellern eigenständig definiert. Auch Novell schließt sich hier mit dem Produkt NetWare/IP nicht aus. Beim UDP-Protokoll kommen die Ports 43981 und 43982 zum Einsatz, jedoch mit der Option, diese bei Verwendung eines primären DSS-Servers anpassen zu können. Zusätzlich verwendet der DSS-Server noch den UDP- und TCP-Port 396. Diese Nummern sind ausschließlich von diesem Dienst zu verwenden. Das DNS von Novell arbeitet nur über UDP und verwendet dort den Standardport 53.

NetWare 5

Da sich der IP-Stack bei der NetWare 5 stark geändert hat und um sehr viele Funktionen erweitert wurde, gibt es hier auch eine deutlich höhere Anzahl von Ports, die verwendet werden. Die Ports für Standarddienste wie DHCP oder DNS entsprechen den Konventionen im IP-Bereich. Nachfolgend finden Sie eine Tabelle mit den NetWare-spezifischen Ports.

Nummer des Zielports	Protokoll	Funktion
524	TCP	NCP-Anforderung einer Quelle oberhalb Port 1024
524	UDP	NCP-Anforderung für die Zeitsynchronisation mit einem Quellport oberhalb 1024
123	UDP	Network Time Protokoll (NTP) für die Zeitsynchronisation, wobei der Quellport die gleiche Nummer hat wie der Zielport
427	UDP	SLP-Anforderung, bei der für die Quelle die gleiche Zielnummer verwendet wird wie für das Ziel
427	TCP	Bei SLP-Anforderungen mit längeren Antworten kommt TCP zum Einsatz anstelle des UDP, auch hier sind Quell- und Ziel nummer identisch.
2302	TCP	Compatibility Mode Driver (CMD), auch gleiche Quell- und Zielnummer
2645	UDP	CMD bei der Kommunikation eines Client über einen Migration Agent, ebenfalls unter Verwendung der gleichen Quell- und Zielnummer

Fenstertechnik

Tips und Tricks zu Windows NT, Teil I

Von Manuel Marsch

Wie erstelle ich einen vollständigen Systembericht unter Windows NT und wie kann ich Windows NT-Dienste restarten? Kann man fremde Ressourcen per IP-Adresse nutzen oder mehrfache IP-Adressen und Hostnamen verwenden? Wie funktioniert das mit den MAC-Adressen unter NT 4.0? Und was bringt das Windows NT Service Pack 4 an Neuerungen? Wir haben einige interessante Tips für Sie zusammengestellt.

Windows NT-Dienste restarten

Zwar ist das Arbeiten mit Windows NT-Diensten auf den ersten Blick recht komfortabel, doch nervt es den Netzwerkadministrator mit der Zeit schon, daß er nach Konfigurationsänderungen einzelne NT-Dienste neu starten, d.h. erst anhalten und dann wieder starten muß. Wem dies über die Diensteverwaltung unter `START / Einstellungen... / Systemsteuerung / Dienste` zu aufwendig ist, der kann dies ganz einfach per Batch über die Kommandozeile oder direkt unter `START / Ausführen`... tun. Folgendes Batch stoppt und startet z.B. den Windows NT-eigenen Webserver (IIS) und kann einfach für andere Aufgaben modifiziert werden:
`RESTART.CMD`:

```
net stop "WWW-Veröffentlichungsdienst"
net start "WWW-Veröffentlichungsdienst"
```

Die Anführungszeichen werden lediglich zur Sicherheit wegen des langen Namens und der Sonderzeichen verwandt und können bei anderen Diensten ggf. weggelassen werden.

Fremde Ressourcen per IP-Adresse nutzen

Sicher kennen Sie den NET USE-Befehl, um unter Windows 9X bzw. Windows NT Verbindungen zu anderen Ressourcen herzustellen. So verbindet z.B. der folgende Befehl `NET USE U: \\SSERVER\HARDDISKC` das lokale Laufwerk `U:` mit der Freigabe `HARDDISKC` des Rechners `SSERVER`. Doch warum muß immer der Rechnername angegeben werden, wenn wir dank Internet doch in der TCP/IP-Welt leben? Keineswegs muß immer ein Rechnername angegeben werden. Lautet z.B. die IP-Adresse o.g. Rechners `194.112.7.8` und ist TCP/IP auf Server und Client korrekt installiert, so funktioniert der Befehl auch mit `NET USE U: \\194.112. 7.8 \HARDDISKC` und Systemadministratoren kennen in der heutigen IP-Welt oftmals IP-Adressen besser als Rechnernamen.

MAC-Adressen unter NT 4.0

Neben logischen Adressen, wie der IP-Adresse, besitzt jede Netzwerkkarte eine Hardware-Adresse, die sogenannte MAC-Adresse, fest eingebrannt. Sie ist weltweit einmalig und wird auf den unteren Kommunikationsschichten verwendet. Doch wie läßt man sich diese unter Windows anzeigen? Windows 95 bietet hierzu das Tool `WINIPCFG`, doch unter Windows NT muß man etwas tiefer einsteigen und in einer Kommandozeile den Befehl `NET CONFIG SERVER` verwenden. Allerdings wird so nur jeweils die eigene Hardware-Adresse angezeigt. Wie jedoch die eines fremden Rechners ermitteln? Ganz einfach: Senden Sie zunächst ein PING auf dessen IP-Adresse: `ping <ip-Adresse>` und lassen sich dann den ARP-Cache Ihres Rechners anzeigen und schon erscheint auch die Netzwerkadresse eines Remote-Clients. TCP/IP verwen-

det nämlich selbst zu Kommunikation mit anderen Hosts die Hardware-Adresse, die bei Ausführung des ping-Befehles automatisch ermittelt und für einige Zeit im lokalen Cache gehalten wird, der dann mittels `arp` ausgelesen werden kann.

Mehrfache IP-Adressen und Hostnamen

Im Gegensatz zu Windows 9X können Windows-NT-PC nicht nur eine, sondern mehrere IP-Adressen an eine Karte binden und unter diesen im Netzwerk verfügbar sein. Diese können einfach neben der primären Adresse unter `START / Einstellungen... / Systemsteuerung / Netzwerk / Protokolle / TCP/IP-Protokoll / IP-Adresse / Optionen` eingetragen werden und stehen Ihnen dann sofort zur Verfügung? Denkste? Im Gegensatz zu allen anderen Änderungen an den Netzwerkeinstellungen, die Windows NT zu einem Restart veranlassen, bleibt die verhaßte Meldung `Computer neu starten` hier aus. Doch ist der PC in den meisten Fällen dennoch neu zu starten, was die Eingabe von `IPCONFIG` in einer Kommandozeile beweist, wenn dort die neuen Adressen nicht gelistet werden. Nach dem nächsten Neustart stehen sie sicher dort.

Anstatt die IP-Adresse zu verwenden, ist es jedoch viel einfacher, einen sprechenden Hostnamen anstelle der kryptischen Adresse zu benutzen, doch wo die verschiedenen Hostnamen eintragen? Unter `START / Einstellungen... / Systemsteuerung / Netzwerk / Protokolle / TCP/IP-Protokoll / DNS / Host-Name:` ist doch nur Platz für einen Hostnamen.

Kein Problem, suchen Sie einfach nach der Datei `Hosts` (meist unter `\WINNT\SYSTEM32\DRIVERS\ETC`) und tragen Sie dort jeweils `IP-Adresse Hostname` für alle relevanten Adressen ein, z.B.:

```
10.1.1.1 Host1
10.1.1.2 Host2
10.1.1.3 Host3
```

Hier können Sie durchaus einer IP-Adresse mehrere Hostnamen zuordnen:

```
10.1.1.1 Host1Name
10.1.1.1 Host2Name
```

Alternativ können Sie alle diese Einstellungen in Ihrem DNS-Server vornehmen, anderenfalls muß die Host-Datei auf alle Rechner Ihres Netzes kopiert werden.

Service Pack 4 Installation

Wie fast jedes Microsoft Windows-Programm bringt auch das Windows NT Service Pack 4 einige interessante Kommandozeilenparameter mit sich, die Sie durch den Aufruf von `UPDATE /?` aufgelistet bekommen. Im einzelnen sind dies:

`-u` unbeaufsichtigter Modus, das Service Pack wird ohne Rückfragen an den Benutzer installiert.
`-f` Beim abschließenden Herunterfahren werden alle Anwendungen ohne Rückfrage geschlossen
`-n` Es wird kein Deinstallationsverzeichnis erstellt.
`-o` Neuere OEM-Dateien werden ohne Nachfrage überschrieben.
`-z` Nach der Installation wird kein abschließender Neustart durchgeführt.
`-q` Die Installation wird ohne Bildschirmausgabe im Hintergrund durchgeführt.

Die Schalter können natürlich beliebig kombiniert werden. So führt z.B. der folgende Aufruf `UPDATE -n -o -z -q` eine stille Installation mit Überschreiben aller Dateien und ohne Neustart durch.

Remote Winsock

Proxies oder Firewalls deaktivieren häufig die DNS-Anschlußnummer 53 (Domain Name System), um externe Standorte davon abzuhalten, die interne DNS-Struktur abzufragen. Dies führt dazu, daß eingehende über Anschluß 53 gesendete Antwortpakete nicht empfangen werden können. SP4 ermöglicht es, die DNS-Serveranschlußnummer von Windows NT zu ändern und für ausgehende Verbindungen eine andere Anschlußnummer zu konfigurieren. Um diese Funktion zu aktivieren, wird in der Registrierung unter `HKEY_LOCAL_MACHINE \Services \Dns \Parameters \SendOnNonDns Port` ein Wert des Typs `DWORD` erstellt. Um eine andere Anschlußnummer als 53 einzustellen, muß dieser Wert von Null verschieden eingestellt werden.

Ist der Wert kleiner als 1024, kann der Server eine beliebige Anschlußnummer verwenden. Ist der Wert größer als 1024, verwendet der Server die angegebene Anschlußnummer.

Neue Ereignisse

Haben Sie das SP4 auf einem Windows-NT-Computer installiert, so erhalten Sie bei jedem Starten dessen in der Ereignisanzeige im `Systemprotokoll (`zu finden unter: `START / Programme / Verwaltung )` ein Ereignis `Systemversion-Ereignis (Ereignis-ID: 6009)`, welches Betriebssystemversion, Built und ServiceLevel angibt und womit nun Systemänderungen nachträglich datierbar sind. Für das Herunterfahren des Systems kommt entweder das Ereignis `Clean Shutdown-Ereignis (Ereignis-ID: 6006)` oder `Dirty Shutdown-Ereignis (Ereignis-ID: 6008)` in Frage. Um einen „dirty Shutdown“ möglichst genau datieren zu können, was sich bei einem Systemabsturz z.B. recht schwierig darstellt, vermerkt Windows NT im laufenden Betrieb alle 5 Minuten einen Zeitstempel, der beim korrekten Herunterfahren gelöscht wird, so daß der „korrupte“ Shutdown beim nächsten Start recht genau datiert werden kann. Wem die 5 Minuten hierzu zu kurz sind, der kann in die Registry unter `HEKEY_LOCAL_MACHINE \Software \Microsoft \Windows \CurrentVersion \Reliability` einen Parameter `TimeStampInterval` vom Typ `DWORD` einfügen, der ein anderes Sicherungsintervall als 5 Minuten angibt. Um diesen Mechanismus zu deaktivieren, tragen Sie hier als Wert einfach `0` ein.

STAND: 12. MAI 1999

Technik-News Patch-CD Juni '99

Empfohlene Novell-Patches

NetWare

NW v5.0
NSSNW5A.exe
NW5SP2.exe
VRPNW5A.exe
NW5NDS1.exe
ODSD.exe
TIMESYNC.exe

NW v4.11
411Y2KP2.exe
ATMDRV03.exe
CHTREE1.exe
DS411Q.exe
DSKDRV.exf
IPX660.exe
IWSP6A.exe
HSTDEV.exe
LANDRV.exe
LDAP103A.exe
IODRV4.exe
MIXMOD3.exe
ODI33F.exe
ODIWAN1.exe
RAD102.exe
RADATR.exe
SCHCMP2.exe
SPXS03A.exe
STRTL6.exe
VRP411a.exe
SCMDA.exe

NW v4.10
410PT8B.exe
410Y2KP2.exe
41REM1.exe
CDUP5A.exe
DS410N.exe
IPX660.exe
LANDRV.exe
LDAPL103.exe
LIBUPI.exe
MAP410b.exe
MIXMOD.exe
NAM41C.exe
NSYNC1.exe
ODI33F.exe
ODIWAN1.exe
SMSUP6.exf
SPXS03A.exe
STRTL6.exe

NW v3.12
312PTD.exe
312Y2KP2.exe
CDUP5A.exe
IPX660.exe
LANDRV.exe
LIB312B.exe
MON176.exe
NAM312.exe
NSYNC1.exe
ODI33F.exe
ODIWAN1.exe
SMSUP6.exe
SPXS03A.exe
STRTL6.exe
TCP312.exe
VRP386.exe

SFT 3 v3.11
311LAN.exe
LIB311b.exe
SFTPT1.exf
SFTUTL6.exe
STRTL6.exe

NW v3.11
311PTG.exe
IPX660.exe
LANDRV.exe
LIB311b.exe
MON176.exe
NSYNC1.exe
ODI33F.exe
ODIWAN1.exe
PBURST.exg
SMSUP6.exe
SPXS03A.exe
STRTL6.exe
VRP386.exe

Tools/Docs
4XMIGR2.exe
CFGRD6B.exe
CONFG7B.exe
COPYNLM3.exe
CRON5.exe
DSDIAG1.exe
ETBOX2.exe
HIGHUTIL1.exe
LOADDLL1.exe
ONSITE5B.exe
STUFKEY5.exe
TABND2.exe
TBACK3.exe
TBOX7.exe
TCOPY2.exe

NetWare Utility Updates

4.10 Utils
41DSVU2.exe
41FILR.exe
41NDIR.exe
MAP412.exe
NETUSR.exe
PS4X03.exe
PU4X03.exe

3.1x Utils
312DU1.exe
BNDFX4.exe
FIL376.exe
MAP312.exe
PS3X02.exe
RCONSOL.exe
SYS376.exe

Server Protocol Updates

NW Mac 312
3XCLNT.bin
ATK307.exe
ATOK31.exf
MACPT3C.exe
MIPXGW.exf
NAM312.exe

NW Mac 410
MACPT3C.exe
NWMAC.exe

MPR 3.1
MPR31B.exe

NLSP-NW 3.12
IPX65g.exe

NLSP-NW 4.10
IPX65g.exe

NW/IP2.2
NIP199.exe
NIP202.exe
NIPW22.exe

NFS 2.1
NFS199.exe

NFS 2.3
NFS205.exe
VXP205.exe

TCP/IP
TCPN06.exe

DHCP SER. 2.0
DHCP21P.exe

Client Kits & Updates

DOS/Win
RPLKT4.exe
TCP16.exe
TLIWS3.exe
VLM121x.exe

APP. Launcher 1.1
NAL111.exe

DOS/WIN32
ADM32.exe
CLTY2KP1.exe
DW26GN.exe
TCP32K.exe

Client LAN DRV
CLTDR2.exf

OS/2
CLOS2N1.exe
OS2PT2.exe

Mac IPX
CTL511.bin
MCLUBD3.bin

Windows 95 dt.
9530IPX.exe
NPTR95.exh
W9530G.exe
W95UNC.exe

Win95 eng.
W9531E.exe

Windows NTdt.
CTLY2KP1.exe
GNNT4111.exe
NA4NTY2K.exe
NTPRINT.exe
NWADMNP1.exe

WinNT eng.
NT411B.exe

ZENwoks Client

Allg. ZEN. Patches
ZW110P2.exe

WIN NT dt.
WNT45G.exe

WIN95/98 dt.
ZW9530G.exe

WIN NT eng.
WNT46E.exe

WIN 95/98 eng.
ZW9531E.exe

Misc. Updates

Bordermana. 2.1
BFC107.exe
BM21Y2K.exe
BMADM2C.exe
BMNW95b.exe
BMNWNTB.exe
BMP107.exe
BMSP2D.exe
BM3NETAD.exe
FILT01A.exe
GBM21Y2K.exe

Bordermana. 3.0
BM3SP1.exe
BMTCPE02.exe

GroupWise 5.2
GW523RC.exe
GW52SP4.exe
GW524USDE.exe
GWCK32A.exe
GW52SP4U.exe
R524USDE.exe

GroupWise 5.5
F32W551A.exe
GW55SP1.exe
GW55SP1U.exe
EXCHNT1.exe

ManageWise v2.1
MWDT07.exe
MWNT01A.exe
MWNXP01B.exe
MWPTN10A.exe
MWVP06A.exe

ManageWi. v2.5/26
MW02B.exe
MWCA1A.exe
MWINOC7R.exe
MWINOC8O.exe
MWNMA3A.exe
MWNMA4A.exe
MWNXP01A.exe
MWNMA26.exe
MW26SP1.exe

NW Connect 2.0
FNWCRNS.exe
NCV20Y2K.exe
NWC206.exe
NWC207.exe
NWC208.exe
NWCMOD.exe
W2N211.exe
NWMP2.exe

LanWork./Group
LWP501.exe
LWP511.exe

NW SAA 2.0
SAA20040.exe

NW SAA 2.1
SAA21030.exe

NW SAA 2.2
MGT22010.exe
SAA22010E.exe

NW SAA 3.0
SAA30010.exe

Lanalyzer 2.2
LZFW01B.exe

SBACKUP
SBACK6.exe

Source Route
SROUTE.exe

Web Server 2.x
WS251C.exe

Web Server 3.x
WS310d.exe

NW for LAT 1.1
LAT002.exe
STAMPD.exe

Empfohlene Microsoft-Patches

Deutsche Updates

Windows 95
D35907.exe
ID4SETUP.exe
W95SP1_G.zip

Windows 98

Windows NT 3.51
SETUPD.exe
SP5351ID.exe

Windows NT 4.0
ID4SETUP.exe
Y2KSP4I.exe

Exchange 4.0
SP4_400I.exe
SP4S400I.exe

Exchange 5.0
SP1_500I.exe
SP1S500I.exe

Englische Updates

Windows 95
IE4USP.exe
IESETUP.exe
MSDUN13.exe
W95PLUSD.exe
W95SP1.exe

Windows 98
Y2K.exe

Windows NT 3.51
IE4USP.exe
SETUPE.exe
SP5_351i.exe

Windows NT 4.0
IE4USP.exe
IESETUP.exe
MPRI386.exe
PPTPFIXI.exe*
RRASFIXI.exe
Y2KSP4I.exe
SP5I386.exe

Exchange 4.0
SP5_400I.exe
SP5S400I.exe

Exchange 5.0
SP2_500I.exe
SP2S500I.exe

Empfohlene AVM Updates und Patches

AVM Produkte für Novell

AVM_MPR_v2.11
M211B05.exe
M211T05.exe

AVM_MPR_v3.0
M30B-06EA.exe

AVM_MPR_v3.1
M31E-11.exe

AVM_Netware_Connect_v1.0
NWCI157A.exe

AVM_NetWare_Connect_v2.0
NWCI2045.exe

AVM Produkte für Microsoft

AVM_MPRI_for_NT
NTR3-R9D.exe

AVM_NDI_for_NT
NDI200.exe

AVM_Access_Server_for_NT
IAS2-R5D.exe

Virtuell_CAPI_95/98/NT
WINNDC33.exe

AVM_NetWAYS_v3.0_W95/98
NW95E-05.exe

AVM_NetWAYS_v3.0_NT
NWNTE-05.exe

AVM_NetWAYS_v4.0
NW40-E02.exe

Empfohlene BinTec Updates und Patches

Bintec Router Software Updates

Bingo!
BGO494.bg

Brick_XS/Office
BRK493.XS
BRK493.XS2

Brick_XM
BRK493.xm
BRK493.xm2

Brick_XL/XL2
BRK493.xl
BRK493 .xl2

Brick_XMP
BRK491.xp

Bingo!_Plus/Professional
BGO494.bgp

BrickWare_u._Configuration_Wizard
BW494P1.exe

Vicas!
VIC494.vc

Empfohlene Tobit Updates und Patches

Tobit Produkte für Novell

Faxware_4.0
FRESHUP.exe
FW_DOS.exe

David_5.0_für_Novell
SP6.exf
ACCOUNT.exe

DAVID_5.2_für_Novell
DVSP2NV.exe
MAILGATE.exe
DVINFO.exe
TLD.exe
PMNW.exe

David_5.11
SP4.exe

FaxWare_5.11_für_Novell
SP4.exe

TimeLAN_Novell
TIMELAN.exe

Tobit Produkte für Microsoft

Faxware_5.11_für_NT
DVSP4.exe

David_5.11_für_NT
DVSP4.exe

David_5.2_für_NT
DVSP2NT.exe
DAVE-MEX.exe
DVINFO.exe
PMNT.exe
SL_NT.exe

Tobit_TimeLAN_für_NT
SETUPNT.exe

Tobit_ServTime_Win_98
SETUPW98.exe

Tobit_ServTime_für_NT
SETUPTI.exe

Inventarliste

Der Bestand und Umfang der Patches auf der Technik News CD verändert sich monatlich. Sobald uns neue Files vorliegen, nehmen wir sie mit auf. Ältere Patches oder solche, die durch neue ersetzt wurden, werden zugunsten neuer Dateien entfernt. (s. `Patches.TXT`)

rot seit unserer letzten Veröffentlichung neu hinzugekommen
grün nur noch auf der Technik News **Service-CD**
blau aus Platzgründen nicht mehr auf der CD

Empfohlene Computer Associates Updates und Patches

ARCserve 6.1 für NetWare

Basis Updates
CAZIPXP.EXE dt/engl.
LO44849.CAZ engl.
AS61SP2.ZIP engl.
AS61SP2G.ZIP dt.
RAAW6146.ZIP engl.
RAAW6146G.ZIP dt.
RAAW6141.ZIP engl.
RAAW6141G.ZIP dt.
AS6UTIL.ZIP engl.

Client und Database Agents:
GroupWise Agent
RAAW6136.ZIP engl.
Open File Agent
NT0237 engl. vorausgs.SP3 für Arcserve für NT 6.0

Client Agent
LO47784.CAZ engl.
RAAW6133.ZIP engl.
RAAW6127.ZIP engl.
RAAW6102.ZIP engl.

Changer Updates
RAAW6143.ZIP engl.
RAAW6147.ZIP engl.
RAAW6143G.ZIP dt.
RAAW6132.ZIP engl.

Disaster Recovery
RAAW6139.ZIP engl.
RAAW6139G.ZIP dt.
RAAW6123.ZIP engl.
RAAW6125.ZIP dt.

Arcserve IT (6.6) für Netware *Enterprise Edtion*

Basis Updates
LO47782.CAZ engl.
LO47527.CAZ engl.vorausgs. LI46307.ZIP engl.

Client und Database Agents:
Open File Agent
AINW0001.ZIP engl.

Disaster Recovery
AINW002.ZIP engl.

Arcserve IT (6.6) für Netware *Workgroup / Single Server / Small Business Edition*

Basis Updates
LO47783.CAZ engl.
LO47528.CAZ engl. vorausgs. LI46307.ZIP

Client und Database Agents:
Open File Agent
AINW0001.ZIP engl.

Disaster Recovery
AINW002.ZIP engl.

ARCserve 6.5 für NT

Basis Updates
LO47027.CAZ engl.
NT0346.ZIP engl.
NT0337.ZIP engl. vorausgs. NT0346
ECN2.ZIP engl. vorausgs. NT0346
NT0321.ZIP engl.
CAZIPXP.EXE dt./eng.
LO43508.CAZ engl.
LO43509.CAZ engl.
LO43511.CAZ engl.
LO43512.CAZ engl.
LO46568.CAZ engl.
LO45984.CAZ engl.
LO43510.CAZ engl.
LO43513.CAZ engl.
NT0363.ZIP engl. vorausgs.NT0346

Client und Database Agents:
Exchange Agent
NT0333.ZIP engl.
LO45986.CAZ engl. vorausgs. LO45984

SQL Agent
LO45987.CAZ engl. vorausgs. LO45984
NT0339.ZIP engl.

Oracle Agent
NT0352I.ZIP engl.
Lotus Notes Agent
NT0340G.ZIP dt.
NT0340.ZIP engl.
SAP R/3 Agent
NT0338.ZIP engl.

Client Agents
LO45985.CAZ engl. vorausgs. LO45984
LO45689.CAZ engl. (+LO45690) vorausgs. ECN2;NT0331
LO45690.CAZ engl vorausgs. LO45689; ECN2;
Lo44254.CAZ engl. NT0331
NT0327.ZIP engl.
RAAW6127.ZIP engl.

Open File Agent
NT0237.ZIP engl.

Complete Options Update
NT0326.EXE engl.
NT0326G.EXE dt.

Tape Library Option
NT0353.ZIP engl.
NT0353G.ZIP dt.

RAID Option
NT0317.ZIP engl.

Image Option
NT0362.ZIP engl.

NT0319.ZIP engl.

Disaster Recovery Option
NT0358.ZIP engl. vorausgs. NT0346
NT0335.ZIP engl.

Die Patches zu ARCserve 6.1 für NetWare, Arcserve IT (6.6) für Netware, ARCserve 6.5 für NT und ARCserve IT (6.6) für NT sind nur für Intel-Maschinen.

dt. = Deutsch engl. = English. vorausgs. = vorausgesetzt

Arcserve IT (6.6) für Windows NT

Basis Updates
LO47525.CAZ engl.
LO47526.CAZ engl.
LO47146.CAZ engl.
LO45992.CAZ engl.
LO45997.CAZ engl.
LO44627.CAZ engl.
REGIT.EXE engl.
CAZIPXP:EXE engl.

Eine Beschreibung der vorab erschienenen Patches findet sich in TN 12/98, TN 4/99 und TN 5/99.

Client und Database Agents:

Exchange Agent	
LO46867.ZIP engl.	vorausgs. LO45992
LO46869.ZIP engl.	vorausgs. LO45997
SQL Agent	
LO46868.ZIP engl.	vorausgs. LO45992
LO46870.ZIP engl.	vorausgs. LO45997
Client Agents	
LO45996.CAZ engl.	vorausgs. LO45992
LO46000.CAZ engl.	vorausgs. LO45997
LO44739.CAZ engl.	
LO44627.CAZ engl.	
Image Options	
AINT0001.ZIP engl.	

Neue Patches in der Übersicht

Novell Updates und Patches neu herausgekommen

NW5SP2.exe 68447 KB
Das Service Pack 2 für die Novell Netware v5.0 ist da, hier die Änderungen und neuen Features im einzelnen:
- beinhaltet die Directory Services v7.30
- alle Änderungen der Patchversion NW5SP1.exe sind enthalten
- Kompatibilität mit der NDS Version 8 gewährleistet
- Installation der NetWare 5 und des Support Pack 2 können parallel ausgeführt werden
- Automatische Installtion des Web Server Updates
- Update der SLP und SCMD Komponenten
- Update der NLS Licensing Files
- Update des TIMESYNC.NLM
- Update der Winsock Dateien

MWINOC7R.exe 11115 KB
Aktuell gibt es diesen Monat wieder einen neuen Client für Managewise 2.5/2.6 für Windows 95. Mit der Release 7R erhalten Sie die Version 4.20 mit dem Build 464.

BMADM2C.exe 4773 KB
Dieses Update enthält ein NetWare Administrator Snap-In für den BorderManager 2.1.

BM3SP1.exe 4672 KB
Hier finden Sie das erste Service Pack für den Novell Bordermanager v3.0.

DS411P.exe 744 KB
In dieser Datei finden Sie ein Update der NDS für die NetWare 4.11, damit sie zusammen mit NetWare 5 Servern in einem Tree betrieben werden kann. Die folgenden Dateiversionen sind enthalten:
DS.NLM v6.03,
DSREPAIR.NLMv4.63,
DSMERGE.NLM v1.63,
DSMAINT.NLM v4.96,
DSVIEW.NLM v1.05,
ROLLCALL.NLM v4.10.

IWSP6A.exe 36706 KB
Im Service Pack 6A für die Novell NetWare 4.11 erhalten Sie Updates für alle Produkte, die der NetWare 4.11 beilegt sind. Desweiteren sind die folgenden Novell Updates bereits enthalten:
UXP205.EXE, IPX65G.EXE, ODI33f.EXE, ODIWAN1.EXE, TCPN05.EXE, VRP411A.EXE, DNS401C.EXE, SBACK6.EXE, SMSUP6.EXE, DS411H.EXE, DHCP21o.EXE, IPX660.EXE, NDB405.EXE, CRON5.EXE, 411Y2KP2.EXE, LIBUPH.EXE, NFS205.EXE, STRTL6.EXE , 41DSVU2.EXE, NIP203.EXE,

ZW110P2.exe 398 KB
In dieser Datei sind die Patches für Novell Z.E.N.Works v1.1 enthalten.

MW26SP1.exe 3139 KB
Service Pack 1 für Novell Managewise v2.6. In diesem Service Pack sind die wichtigsten Patches für Managewise v2.6 zu einem Service Pack zusammengefaßt.

MWINOC8O.exe 7884 KB
Für den Managewise 2.5/2.6 Client für Windows NT hat Novell ein neues Service Pack bereitgestellt. Darin enthalten ist wie immer auch ein aktuelles Viren-Update. Die Version des Clients erhöht sich durch das Service Pack auf 4.20.

EXCHNT1.exe 3746 KB
In diesem File finden Sie den Patch 1 für das Exchange Gateway für Groupwise v5.5.

BMTCPE02.exe 336 KB
Das neue TCPIP.NLM (Version 5.02) für den Einsatz auf Netware 4.11 und 5.0 ist speziell für den Novell Bordermanager v3.0. Es ist auch nur in Verbindung mit dem Novell Bordermanager getestet und entsprechend zu verwenden.

NWMAC.exe 1363 KB
NetWare for Macintosh Version 4.x für den Einsatz unter Novell NetWare 4.2 wird mit Ablauf des 30 April im Jahr 2000 nicht mehr supported.

Tobit Updates und Patches neu herausgekommen

PMNT.exe

Dieses aktualisierte Version des David PostMan (POSTMAN.EXE) setzt eine installierte Version von David 5.2 für Windows NT (Programm CD vom 01.Februar 1999 oder Service Pack 2) voraus. Diese Version ist nicht im aktuellen Service Pack enthalten. In der bisherigen Version konnte es bei bestimmten Providern vorkommen, daß nur dann E-Mails versendet werden konnten, wenn vorher E-Mails empfangen wurden.

PMNW.exe

Dieses Download enthält eine aktualisierte Version des David PostMan für NetWare (POST MAN.NLM). Der Einsatz dieses Moduls setzt eine installierte Version von David 5.2 (Programm CD vom 01.Februar 1999 oder Service Pack 2) voraus! Diese Version ist ebenfalls nicht im aktuellen Service Pack enthalten. In der bisherigen Version konnte es bei bestimmten Providern vorkommen, daß nur dann E-Mails versendet werden konnten, wenn vorher E-Mails empfangen wurden.

DVINFO.exe

Das Windows Utility DVINFO.EXE durchsucht nach dem Aufruf die Arbeitsstation nach Dateien des David Clients und zeigt diese in einer Listbox an. Die Liste enthält die ermittelte Versionsnummer, Dateigröße, Datum und Verzeichnispfad jeder einzelnen Datei. Zusätzlich enthält die Liste auch Informationen fremder Dateien, die vom David Client verwendet werden (z.B. UNIDRV.DLL, NWIPXSPX.DLL). Sofern eine Datei geladen ist, wird dies durch ein Sternchen (*) vor dem Dateinamen angezeigt. Auf Wunsch kann die Liste als Textdatei abgespeichert werden.

TLD.exe

Das Download enthält den aktuellen TLD (Transport Layer Driver) für den Betrieb von Siemens M20 GSM Modems mit David/Tobit FaxWare unter Novell NetWare.
Diese Version ist für das genannte Modem zwingend notwendig, kann aber auch für das Siemens M1 GSM Modem verwendet werden.

DAVE-MEX.exe

Dieses Gateway zu Microsoft Exchange für David und Tobit FaxWare bildet die vollständige und nahtlose Schnittstelle für den Empfang und den Versand von Nachrichten.
Es erfordert einen Server unter Windows NT 4 mit installiertem Service Pack 3.
Die Installation des Gateways muß auf dem NT Server erfolgen (Primary Domain Controller, Backup DC oder Stand Alone Server), auf dem auch Microsoft Exchange installiert ist.
David bzw. Tobit FaxWare muß auf dem gleichen Server oder einem Remote Server im Netz installiert sein (NetWare oder NT).
Die folgenden Neuerungen sind in der aktuellen Version enthalten:

- Versenden und empfangen von E-Mails mit Attachment
- Neuer Parameter, um das Polling-Intervall festzulegen, in dem nach neuen Nachrichten gescannt wird (siehe aktuelle Dokumentation)
- Adreßübergabe bei eingehenden Nachrichten
- Übertragung der Systemmeldungen vom David-Server wird unterbunden.
- kann durch neuen Schalter in der Dave/MEX Konfiguration wieder aktiviert werden.
- E-Mail Versand an Adressen aus dem globalen Adreßbuch des Exchange-Servers (Benutzerdefinierte Empfänger Adressen)

MAILGATE.exe

Das Download enthält ein MailGate NLM, das auch mit FaxWare 5.2 eingesetzt werden kann, einen neuen Service Layer (DAVID.NLM) sowie ein neues POSTMAN.NLM. Zusätzlich ist jeweils ein neuer Fax-Image Druckertreiber für Windows NT, 95/98 und 3.x enthalten. Diese Module können nicht mit David 5.0/David 5.11 oder „Tobit FaxWare für NetWare for Small Business 4.2“ verwendet werden!
Für den Betrieb dieser Versionen muß das aktuelle Service Pack 2a von David/FaxWare 5.2 bzw. die Programm CD vom 01.Februar 1999 installiert sein. Außerdem muß ein PostMan Port bereits eingerichtet sein bzw. anschließend eingerichtet werden. Hierzu muß eine freie Port-Lizenz in der Lizenzdatenbank eingetragen sein. Wenn Sie bereits eine frühere Version von MailGate 2 installiert haben, wird diese automatisch aktualisiert.
Es gibt folgende Neuerungen:

- MailGate 2 kann nun auch mit FaxWare 5.2 eingesetzt werden
- Neuer Fax-Image Druckertreiber (Windows NT, 95, 3.x) unterstützt die FaxWare Befehle (@@-Befehle)
- Einfügen von Include Dateien, um z.B. per FaxWare Befehl ein Deckblatt vorzuschalten
- Empfangene Faxdateien können als PCX oder GIF Datei an eine E-Mail angehängt werden
- Subjekt in Deckblättern funktionierte nicht korrekt

Microsoft Updates und Patches neu herausgekommen

SP5I386.exe 34553 KB

Service Pack 5 für Windows NT 4.0 (englisch).

Computer Associates Updates und Patches neu herausgekommen

Arcserve 6.5 für NT

Lo47027.CAZ

Voraussetzung für diesen Patch ist, daß Sie die Patches LO45690 und LO45689 zuerst für alle NT Agents einsetzten.
Er enthält folgende Fixes:

LO43508 – Tapecopy kann die Band Sequence nicht wiederfinden.
LO43509 – Unbeaufsichtigte Installation überschreibt die Datenbank und Jobqueue.
LO43511 – Benutzer ohne Admin Rechte können ARCserve nicht verwenden.
LO43512 – Die Ausdünnungs-Informationen wurden überschrieben.
T683186 – Exchange Backup funktioniert nicht, wenn es im GFS-Schema verwendet wird.
T683188 – GPF (Dr. Watson) in ASRUNJOB.EXE während des Sicherns oder Wiederherstellens.
T683192 – Falscher Eintrag in Registry .
T683196 – TMP-Dateien wurden nicht zu CAT-Dateien geändert.
T683197 – CAT wurden nicht in Datenbank eingefügt.
T683198 – Band wurde nicht wiederverwendet, wenn es im Scratch Set war.
T683199 – SQLDBSP1.EXE
T683200 – Unterstützung für ASJBSTAT.DLL für TNG Workload Komponente.
T683202 –GP (Dr. Watson) trat beim Wiederherstellen von NT auf NetWare auf.
T683204 – Probleme mit TAPEENG,wenn über ARCserve Kommandos vor dem Backup ausgeführt werden.
T683206 – Es konnten keine Files vom Wiederherstellungs-Fenster gesehen werden.
T683208 – Mit einem WANGDAT 3400 konnte nicht gesichert werden.
T683210 – Cluster Unterstützung.
TFF2002 – Freigaben (C$,D$)wurden mehrmals dargestellt.
TFF2007 – Falsche Anzahl von Dateien wurde bei großen Datenmengen migriert.
TFF2014 – ARCServe Ereignisse wurden nicht in das NT Event Log eingetragen.
TF75026 – SQL-Einfügen funktionierte nicht nach Ausdünnen.
T146148 – Keine Sicherheitsabfrage beim Purge Utility.
T11C002 – GFS Steuerung hatten keinen Job für nächsten Tag.
T11C007 – Ein Backslash wurde zum SQL Job Script zugeführt, wenn es verändert wurde.
TF75025 – Wiederherstellungs Problem mit Ereignisprotokoll.
T167002 – Wurde das GFS Schema so geändert, daß es anhängen sollte, konnte dies nicht gesichert werden.
T167003 – Es konnte der Ort für die Bänder bei entfernten Servern nicht geändert werden.
T683227 – Verbesserte Performance beim Ausdünnen der ARCserve SQL Datenbank.
LO46568 – Zusätzliche Streamer Unterstützung.
LO45689 – Sicherheits-Protokollerweiterungen.
T683238 – Man konnte im Wiederherstellungs-Fenster die NetWare Dateien nicht sehen.

ArcserveIT 6.6 für NT:

Lo47525.CAZ

Durch diesen Patch werden zusätzlich Onstream-Laufwerke in der Enterprise Version unterstützt.

Lo47526.CAZ

Wie vorher, nur für die Workgroup Version.

Lo47146.CAZ

Durch diesen Patch werden folgende Laufwerke unterstützt.
SONY DMS-B35
Exabyte EZ17 Library
SONY DMS-B35 Library
Exabyte 690D Library
COMPAQ TL895 Library
Tandberg DLT 4000 und DTL 7000 Laufwerke
HP C5683A Drive
Folgende Probleme werden behoben:
Informationen der Bänder in die Datenbank zurückzulesen, funktionierte nicht, wenn sie über zwei Bänder gingen und ein NS8 von Tandberg beteiligt war. Bei der automatischen Konfiguration mit der IBM 3570 Library kam es zu einem Problem. Dieser Patch ersetzt den Fix LO44627.

ArcserveIT 6.6 für Novell:

Enterprise Edition

Lo47782.CAZ

Mit diesem Patch wurde ein erweitertes Sicherheitsprotokoll zwischen dem NT Client Agent und dem ARCserve Manager eingeführt.

Lo47527.CAZ

Dieser Patch verhindert einen Abend des Intrleav.NLM beim Sichern eines entfernten Servers mit dem Push-Agent. ARCserve kann keine Daten von Bändren zurücksichern, die schon mit ARCserve 6.1 verwendet wurden. Dieses wurde mit DLT, AIT oder Exabyte 8900 Laufwerken beobachtet. Sie müssen vorher das Service Pack 2 eingespielt haben.

Workgroup /Single Server / Small Business Edition

Lo47783.CAZ (Lo47783.ZIP)

Mit diesem Patch wurde ein erweitertes Sicherheitsprotokoll zwischen dem NT Client Agent und dem ARCserve Manager eingeführt.

Lo47528.CAZ

Dieser Patch verhindert einen Abend des Intrleav.NLM beim Sichern eines entfernten Servers mit dem Push-Agent. ARCserve kann keine Daten von Bändren zurücksichern, die schon mit ARCserve 6.1 verwendet wurden. Dieses wurde bei DLT, AIT oder Exabyte 8900 Laufwerken beobachtet. Sie müssen vorher das Service Pack 2 eingespielt haben.

Durch den Draht geschaut

Teil VI: Das NetWare IPX/SPX

Von Jörg Rech

Nachdem wir uns in den letzten Ausgaben der Technik News mit den Protokollen für die Client-Server Kommunikation im Microsoft Netzwerk und Novell-Netzwerk beschäftigt haben, möchten wir nun mit den Transportprotokollen fortfahren. Beginnen wollen wir dabei mit den NetWare Protokollen IPX und SPX.

Stellen die oberen Protokolle von der fünften bis zur siebten Schicht des OSI-Referenzmodells die eigentliche Kommunikation innerhalb des Netzwerks dar, so sind die Protokolle der dritten und vierten Schicht für den Transport der Daten zuständig. Laut Definition ist dabei die dritte Schicht des OSI-Referenzmodells, die Netzwerkschicht, unter anderem für die Wegfindung, den Aufbau, das Aufrechterhalten und das Beenden einer Verbindung zu einem entfernten System verantwortlich. Die vierte Schicht im OSI-Referenzmodell, die Transportschicht, stellt sicher, daß die Teile der Daten in der Reihenfolge abgeliefert werden, in der sie gesendet wurden. Dazu bedient man sich verschiedener Protokolle, die zur Realisierung der Datenübertragung zusätzliche Informationen enthalten. Diese Informationen werden beim Senden einfach vor die eigentlich zu übertragenden Daten der höheren Schichten gesetzt. Empfangsseitig werden diese vorgesetzten Protokollinformationen wieder entfernt, so daß die Daten der höheren Schicht übrig bleiben.

Wegfindung

Warum benötigt man eigentlich für den Transport der Daten zusätzlich ein Transportprotokoll, und warum sind nicht die Adreßinformationen des MAC-Headers ausreichend? Betrachtet man ein Netzwerk genauer, so stellt man fest, daß es normalerweise

aus mehreren Teile besteht, die über Router miteinander verbunden sind. Möchte man nun Daten zu einer Station verschicken, die sich auf einem anderem Netzwerk befindet, so müssen diese Daten in irgendeiner Form adressiert werden können. Dazu werden in den Protokollen der dritten Schicht die Netzwerkadresse der Zielstation und die eigene Netzwerkadresse eingetragen. Auf der zweiten Schicht werden als Ziel die MAC-Adresse des Routers und die MAC-Adresse der sendenden Station eingetragen. Die Station sendet also über die Adressierung auf der MAC-Ebene ihre Daten erst einmal zum Router. Der Router entfernt den MAC-Header und verschickt die Daten entweder zu einem benachbarten Router oder wenn der Router auf der anderen Seite an das Zielnetzwerk anschließt, direkt an die Zielstation. Die Wegfindung für die Versendung der Daten zu einer entfernten Station wird dabei vor der Versendung der Daten über spezielle Routing-Protokolle oder statische Routing-Tabellen bestimmt (vgl. Abb. 1).

Der MAC-Header alleine würde in diesem Fall nicht ausreichen, denn über die Adreßinformationen des MAC-Headers alleine lassen sich nur Stationen adressieren, welche sich auf demselben Netzwerk befinden.

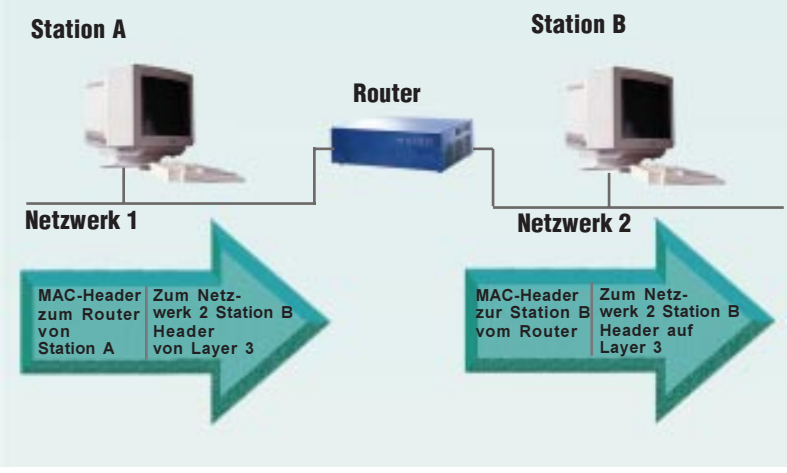
Erst durch die zusätzliche Adressierungsmöglichkeit lassen sich Netzwerke mit mehreren Netzwerkteilen aufbauen und die Daten beliebig zwischen den gekoppelten Netzwerken transportieren, siehe Abb. 1.

Sichere Kommunikation

Bei einer Datenübertragung unterscheidet man grundsätzlich zwischen einer verbindungslosen und einer verbindungsorientierten Kommunikation. Dabei haben beide Verfahren jeweils ihre Vor- und Nachteile, welche von Fall zu Fall abgewägt werden müssen. Eine verbindungslose Kommunikation läßt sich mit der Versendung eines einfachen Briefes vergleichen. Man wirft einen Brief in den Briefkasten und hofft, daß er Brief irgendwann einmal beim gewünschten Empfänger ankommt. Erhält man Tage später einen Anruf, daß die Sendung nicht ankam, hat man einige Zeit verloren, bis man das erfahren hat, zudem muß man neu schreiben. Ist man jedoch von Anfang an bereit, höhere Portokosten in Kauf zu nehmen, so bietet sich als Alternative, den Brief per Einschreiben zu verschicken, was mit der verbindungsorientierten Kommunikation vergleichbar ist. Man erhält eine Quittung. Ist der Brief nicht zustellbar, erhält man ihn zurück und ist ebenfalls über die mißglückte Zustellung informiert. Andernfalls kann man davon ausgehen, daß er ordnungsgemäß angekommen ist.

Wie bei der Briefzustellung verwendet man im Netzwerkbereich gesicherte und ungesicherte Mechanismen für die Versendung der Daten. Wobei die gesicherte der verbindungsorientierten Kommunikation entspricht, die in der Regel mit einem erhöhten Protokoll-Overhead bezahlt werden muß, was aber andererseits für eine verläßliche Übertragung der Daten sorgt. Die verbindungslose Kommunikation hingegen hat einen geringeren Protokoll-Overhead. Die gesicherte Datenübertragung muß dann von den höheren Protokollschichten gewährleistet werden. Es sei denn, man hat eine gewisse Form der Datenübertragung, bei der keine gesicherte Zustellung maßgebend ist oder nicht sinnvoll realisiert werden kann.

Abb. 1: Zuordnung der höheren Protokolle, die entweder das IPX oder das SPX für den Transport nutzen.


Station A
Station B
Router
Netzwerk 1
Netzwerk 2
MAC-Header zum Router von Station A
Zum Netzwerk 2 Station B Header von Layer 3
MAC-Header zur Station B vom Router
Zum Netzwerk 2 Station B Header auf Layer 3

Novells Protokollwelt

Novell bietet für den Datentransport zwei hauseigene Protokolle, Internetwork Packet Exchange IPX und Sequenced Packet Exchange SPX. Dabei ist IPX auf der dritten Schicht des OSI-Referenzmodells anzusiedeln, SPX auf der vierten. Bei dieser Aussage werden Kritiker sagen, daß die Zuordnung nicht ganz richtig ist. Stimmt, betrachtet man sich die IPX- und SPX-Header genauer, so stellt man fest, daß bei einem SPX-Header der Anfang des Headers dem des IPX-Headers entspricht und SPX letztendlich eine Erweiterung des IPX-Headers darstellt (siehe Abb. 3 und Abb. 4). Man müßte somit bei einer genauen Betrachtung sagen, daß das SPX-Protokoll auf die dritte und vierte Ebene des OSI-Referenzmodells zuzuordnen ist. Dies wird deutlich, wenn man sich ein SPX-Datenpaket mit dem LANalyser betrachtet, wo es im Summary-Fenster in einen IPX- und einen SPX-Teil gegliedert ist.

Pure IP versus IPX

In der Vergangenheit sind die Protokolle IPX/SPX im Zusammenhang mit der NetWare ein klares Muß gewesen, da das NCP, das in einem Novell-Netzwerk für die Client-Server Kommunikation genutzt wird, IPX/SPX vorausgesetzt hat. Innerhalb heutiger Netzwerke verliert jedoch

das IPX/SPX immer mehr an Bedeutung. Denn heutzutage haben in der Regel die Netzwerke einen Zugang zum Internet und benutzen bevorzugt TCP/IP als Transportprotokoll. Daß IPX/SPX an Bedeutung verloren hat, wird an der Einführung von Pure IP in Novells NetWare5 deutlich, die es dem NCP ermöglicht, direkt auf TCP/IP aufzusetzen. Allerdings setzt der Einsatz von TCP/IP eine detaillierte Kenntnis über die Vergabe von Netzwerkadressen und die Bildung von Subnets voraus.

Novells IPX hingegen hat eine Art Plug-and-Play-Adreßmechanismus, in dem jeder Station automatisch eine eindeutige Adresse zugeordnet wird, also ohne daß aufwendige Adreßkonfigurationen an den einzelnen Stationen im Netzwerk vorgenommen werden müßten. In einem Novell-Netzwerk ohne Internet-Zugang bietet somit IPX/SPX auch zu Zeiten der NetWare5 eine gute Alternative, die in der Konfiguration weitaus weniger Kenntnis voraussetzt und zusätzlich durch einen geringeren Protokoll-Overhead gegenüber TCP/IP letztendlich auch das schnellere Transportprotokoll darstellt.

Man sollte aber auf jeden Fall vermeiden, daß parallel mehrere Transportprotokolle installiert werden, da dies in einem Netzwerk, in dem NetWare-Server und Windows-Betriebssysteme eingesetzt werden, dazu führen würde, daß viele Dienste parallel für jedes zusätzlich installierte Protokoll eigenständig ausgeführt werden. Parallel installierte Protokolle würden somit unweigerlich zu einer unnötigen Verschwendung der verfügbaren Bandbreite führen und die Gesamt-Performance des Netzwerks negativ beeinflussen.

IPX

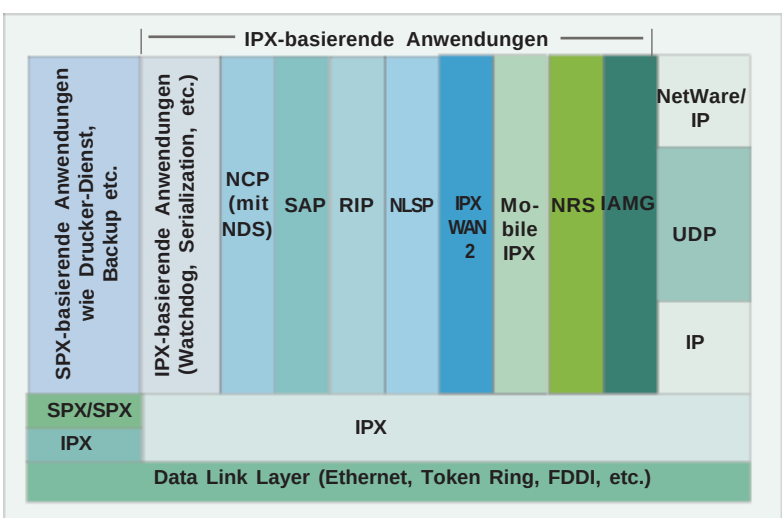
Gegenüber SPX hat IPX den Vorteil, daß der Protokoll-Overhead geringer ist. Jedoch muß dies mit dem Risiko einer verbindunglosen Kommunikation bezahlt werden, wobei es keine Garantie gibt, ob die Daten beim Empfänger ordnungsgemäß und in der richtigen Reihenfolge, sprich richtigen Sequenz, eingetroffen sind. Zum größten Teil wird bei der NetWare-Kommunikation auf die Kontrollinstanz der Transportprotokolle verzichtet. Das NCP stellt selbst ein verbindungsorientiertes Protokoll dar, somit kann in diesem Fall auf die Kontrolle der Transportprotokollebene verzichtet werden. Man verschiebt in diesem Fall die Kontrollinstanz einfach auf die höhere Protokollebene. Das hat wiederum den Nachteil, daß bei einer fehlerhaften Kommunikation, falls ein Teil der Daten verlorengegangen ist, die erneute Versendung der Daten viel aufwendiger ist und ein System mehr belastet. Es gibt jedoch auch Arten der Kommunikation, wie das Service Advertising Protocol SAP, das einer broadcast-adressierten Ankündigung eines Dienstes entspricht, in der eine verbindungsorientierte Kommunikation gar nicht möglich wäre. Denn eine Kontrolle mit einem unbekannten Ziel läßt sich schlicht und einfach nicht durchführen, siehe Abb. 2.

IPX-Header

Der IPX-Header hat eine Länge von 30 Bytes und beinhaltet 10 Felder. In den Feldern sind unter anderem Informationen über die Länge, die passierten Router, die Netzwerkadresse und Knotenadresse der Zielstation enthalten. Das erste Feld des IPX-Headers ist das Feld `Checksum` mit einer Länge von 2 Bytes. Es hat in der Regel den Inhalt `0xFFFF`. Mit dem Checksummen-Feld kann auf Wunsch eine Überprüfung des IPX-Headers durchgeführt werden. Per Standardeinstellung ist auf Seiten der Clients und Server die IPX-Checksummenkalkulation abgeschaltet, da sie sich grundsätzlich auf die Performance negativ auswirkt. Novell vertritt in diesem Fall die Meinung, daß die Fehlerüberprüfung anhand der CRC-Überprüfung, welche Bestandteil jedes Frametyps ist, ausreichend ist. Besteht man jedoch auf erhöhter Sicherheit, läßt sich die IPX-Checksummenkalkulation client- und serverseitig aktivieren, es sei denn, man verwendet das Ethernet_802.3 Frame-Format, da hier die `0xFFFF` am Anfang des IPX-Headers für die eindeutige Kennung eines IPX-Paketes benötigt werden. Das zweite Feld `Length` enthält die Angabe über die gesamte Länge des Internetwork-Paketes, also die Länge des IPX-Headers und die Länge des darauffolgenden Datenteils.

Das Feld `Transport Control` kennzeichnet die Anzahl der Router, die ein IPX-Paket auf dem Weg von der Quelle bis zum Ziel insgesamt passiert hat. Dieses Feld hat eine Länge von einem Byte, es läßt somit einen Wertebereich von 0 bis 15 zu. Beim Aussenden eines IPX-Paketes wird der Wert von der sendenden Station auf Null gesetzt. Jeder Router, der passiert wird, erhöht den Wert um Eins. Nach dem 15ten Router ist der Wert auf 15 gesetzt und stellt somit

Abb. 2: Durch die zusätzlich gewonnenen Adressierungsmöglichkeiten lassen sich Daten über die Grenzen eines Netzwerks transportieren.



den maximalen Wert des Feldes dar. Wird versucht, einen zusätzlichen Router zu passieren, wird das Paket einfach verworfen. Hierin liegt begründet, daß ein Novell-Netzwerk mit maximal 15 Routern aufgebaut werden kann, einen höheren Wert läßt das Transport Control Feld des IPX-Headers schlicht und einfach nicht zu. Bei der Festlegung der Anzahl der passierten Router spricht man auch von der Anzahl der Hops beziehungsweise einem Hop-Counter.

Typ und Adressierung

Das nächste Feld mit der Bezeichnung `Packet Type` gibt den vom Paket genutzten Service Typ an. Der Wert 0 oder 4 entspricht dabei der IPX-Kommunikation, der Wert 5 einer SPX-Kommunikation und der Wert 17 der NCP-Kommunikation. Das Feld stellt somit die Kennung des Pakettyps dar. Das Feld `Destination Network` gibt die 4 Byte lange Netzwerkadresse des Netzwerkes an, in dem sich die Zielstation befindet. Der Wert `0x00-00-00-00` entspricht der Adressierung einer Zielstation, welche sich im selben Netzwerk wie die sendende Station befindet. Dieses Paket wird deshalb grundsätzlich auch nicht über Router weitergeleitet. Wird ein Paket zu einem Novell-Server verschickt, so beinhaltet dieses Feld die interne Netzwerkadresse des Servers. Bei dem darauffolgenden 6 Byte langen `Destination Node` Feld, handelt es um die Adresse der Zielstation. In einem als Broadcast adressierten Paket beinhaltet dieses Feld den Wert `0xFF-FF-FF-FF-FF-FF`. Wird ein Paket an einen Server verschickt, so enthält das Destination Node Feld die Adresse 0x00-00-00-00-00-01 und wird somit vom NetWare Protocol Stack auf das interne IPX-Netzwerks des Servers zugeordnet.

Das folgende Feld `Destination Socket` hat eine Länge von 2 Bytes und kennzeichnet mit seinem Wert den Endprozeß, der als Socket bezeichnet wird, für den das Paket letztendlich bestimmt ist. Beispielsweise entspricht der Wert `0x0451` dem des NCPs (weitere Werte siehe Tabelle 1).

Sockets

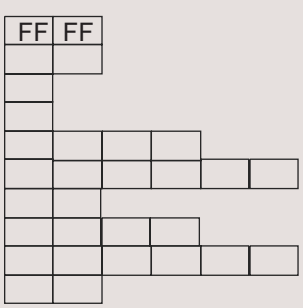
Bei den Sockets unterscheidet man grundsätzlich zwischen den Well-Known Sockets, den dynamischen Sockets und den Sockets für Drittanbieter. Die Well-Known Sockets entsprechen den Sockets, die von Novell fest vergeben wurden. Dynamische Sockets werden von den Clients benutzt, um ihre Prozesse eindeutig zu kennzeichnen. Ein Client kann dadurch parallel mehrere offene Prozesse haben, also Prozesse, die noch nicht vollständig abgearbeitet wurden. Der Server benutzt bei der Kommunikation mit dem Client dieselbe Socket-Nummer, damit der Client die Antwort des Servers eindeutig zu seinem Prozeß zuordnen kann. Für die Dynamischen Sockets ist der Bereich von `0x4000` bis `0x8000` freigegeben, die Dynamische Socket-Nummer wird vom Client über einen Zufallsgenerator generiert und festgelegt.

Den Wertebereich von `0x8000` bis `0x9000` hat Novell für Drittanbieter vorbehalten, so hat beispielsweise die Firma Oracel sich die Socket-Nummern `0x807F`, `0x8080` und `0x8081` zuordnen lassen. Sie sind somit in der Lage, ihre Kommunikation eindeutig zu kennzeichnen und damit anzuzeigen, daß es sich hierbei um keine NCP Kommunikation handelt. Auch Hersteller von netzwerkfähigen Games benutzen bestimmte Socket-Nummern, um eine spezielle Kommunikation, welche für das Game Performance optimiert ist, zu kennzeichnen und nutzen zu können.

Das Feld `Source Network` enthält die Adresse des Netzwerks, auf dem sich die sendende Station befindet. Bei einem Paket, das von einem Server gesendet wurde, entspricht der Inhalt des Source Network Felds der internen IPX-Adresse des Servers. Bei dem Feld `Source Node` handelt es sich um die 6 Byte lange Knotenadresse der Quell-Station. Die Adresse `0x00-00-00-00-00-01` entspricht dabei einem Paket, dessen Ursprung ein NetWare Server war. Im letzten Feld des IPX-Headers, dem `Source Socket` Feld, wird die Socket-Nummer des sendenden Prozesses angegeben, wobei die Festlegung der Werte dem der Destination Sockets entsprechen, siehe Abb. 3.

Socket-Nummer	Socket
0x0451	NCP NetWare Core Protocol
0x0452	SAP ServiceAdvertising Protocol
0x0453	RIP Router Information Protocol
0x0455	NetBIOS
0x0456	Diagnostic Responder (Diagnosepaket)
0x0457	Serialisation (Serialisierungspaket)

Tab. 1: Sogenannte Well-Known Sockets, die von Novell festgelegt wurden.



2 Bytes	IPX Checksum
2 Bytes	Length
1 Byte	Transport Control
1 Byte	Packet Type
4 Bytes	Destination Network Adress
6 Bytes	Destination Node Adress
2 Bytes	Destination Socket Number
4 Bytes	Source Network Adress
6 Bytes	Source Node Adress
2 Bytes	Source Socket Number

Abb. 3: Zeigt den Aufbau des IPX-Headers

Aufschlüsse

Für die Protokollanalyse sind die Adreßinformationen des IPX-Headers

von großer Bedeutung, da nur sie die Quelle und das Ziel eindeutig kennzeichnen. Denn man muß berücksichtigen, daß sich die Adreßinformationen des MAC-Headers automatisch verändern, sobald die Daten einen Router passiert haben. Weiterhin lassen sich anhand des Hop-Count innerhalb des Transport Controll Felds die Anzahl der Router ermitteln, welche die Daten auf dem Weg von der Quelle zum Ziel passiert haben. Mit Hilfe dieser Information lassen sich unter Umständen Optimierungen im Netzwerk durchführen, indem Stationen, die häufig miteinander kommunizieren, näher zusammengebracht oder in dasselbe Netzwerk verlegt werden.

Eine möglicherweise irrtümlich aktivierte Checksummenkalkulation an einer der Stationen im Netzwerk, läßt sich ebenfalls anhand der während der Protokollanalyse gewonnen Informationen ermitteln. Hier liegt möglicherweise die Ursache für eine langsam kommunizierende Station im Netzwerk.

Über die Informationen der Socket Number kann der Kommunikationsanteil im Netzwerk bestimmt werden, beispielsweise wer und wie oft Zugriffe auf einer Oracel-Datenbank tätigt. Außerdem lassen sich Mitarbeiter ausfindig machen, welche einen Teil ihrer Arbeitszeit nutzen, um über das Netzwerk IPX-basierende Spiele mit Kollegen zu spielen.

Neu und Alt

Historisch bedingt gibt es bei dem SPX-Protokoll zwei verschiedene Versionen, die als SPX und SPX-II bezeichnet werden. Erstmalig wurde das neue SPX-II 1992 auf der Novell Developer Conference von Novell vorgestellt. Die erste Version des SPXs ließ nur eine maximale Paketgröße von 576 Bytes zu. Da alleine der SPX-Header eine Länge von 42 Bytes hatte, konnten somit maximal 534 Bytes an Nutzdaten übertragen werden.

Diese Längenrestriktion hatte ihren Ursprung im Xerox Networks System XNS und war bei der ARCnet-Technologie nicht so dramatisch, da sowieso nur die Übertragung von 508 Bytes Nutzdaten möglich war. Zu Zeiten von Ethernet, Token-Ring oder FDDI war diese Längenrestriktion für den Austausch großer Datenmengen natürlich nicht mehr tragbar. Somit war Novell gezwungen, die Längenbeschränkung des SPX-Protokolls zu beseitigen. Das Ergebnis war die Einführung von SPX-II, was die verfügbaren Datenlängen der neuen Netzwerktechnologien unterstützen konnte und mit zusätzlichen Verbesserungen aufwartete.

SPX-Header

Bei dieser Folgeversion SPX-II wurde der Aufbau des Headers durch ein zusätzliches Feld, das an den bestehenden SPX Header angehängt wurde, etwas erweitert. Das neue Feld hat eine Länge von 2 Bytes, so daß die gesamte Länge des neuen SPX-II Headers 44 Bytes beträgt. Bei einem großen Teil der heutigen verbindungsorientierten Kommunikation wird jedoch immer noch das Standard SPX verwendet, da dessen Datenlänge in vielen Fällen ausreicht. Die ersten 42 Bytes sind bei beiden SPX-Versionen identisch, wobei es sich bei den ersten 30 Bytes um die Datenfelder des IPX-Headers handelt. Der SPX-Header wird durch den Wert `0x05` im Paket Type Feld innerhalb des IPX-Teils gekennzeichnet.

Die gegenüber dem IPX-Header zusätzlich vorhandenen Felder werden letztendlich für die Kontrollmechanismen, welche für eine verbindungsorientierte Kommunikation benötigt werden, genutzt. Unter anderem beinhalten die zusätzlichen Felder des SPX-Teils das 1 Byte lange `Connection Control` Feld, das den Datenaustausch steuert. Der Wert `0x10` symbolisiert beispielsweise, daß die Datenübertragung beendet wird. Beinhaltet das Connection Control Feld den Wert `0xC0`, so handelt es sich um ein Systempaket mit einer Bestätigung oder mit einer Anforderung für eine Bestätigung (weitere Definitionen siehe Tabelle 2).

Das folgende Feld `Datastream Type` hat eine Länge von 1 Byte und kennzeichnet den Datentyp, welcher in dem Paket transportiert wird. Der Wertebereich von `0x00` bis `0x7F` ist dabei für Anwendungen reserviert, der Bereich von `0x80` bis `0xFD` ist für SPX-II reserviert. Die letzten zwei möglichen Werte sind speziellen Aufgaben zugeordnet, wobei der Wert 0xFE das Ende eine Verbindung angibt und der Wert 0xFF die Bestätigung für den Verbindungsabbau signalisiert.

Bit-Position	Bezeichnung	Bedeutung
Bit 0	XHD	Reserviert für SPX-II, kennzeichnet, daß ein erweiterter SPX-II Header verwendet wird
Bit1	RES1	Reserviert, muß immer auf Null gesetzt sein
Bit2	NEG	Festlegung, ob es sich um eine SPX-II Anforderung oder eine Antwort handelt, bei SPX ist dieser Wert immer auf Null gesetzt
Bit3	SPX-II	Kennzeichnet ein SPX-II Paket, ist bei SPX auf Null gesetzt
Bit4	EOM	Ende einer Nachricht
Bit5	ATN	Kennzeichnet ein Paket mit erhöhter Aufmerksamkeit, ist bei SPX auf Null gesetzt
Bit6	ACK	Anforderung für eine Bestätigung
Bit7	SYS	Systempaket, wird als Bestätigung verwendet

Tab. 2: Festlegung der einzelnen Bits des Connection Control Felds im SPX bzw. SPX-II Header

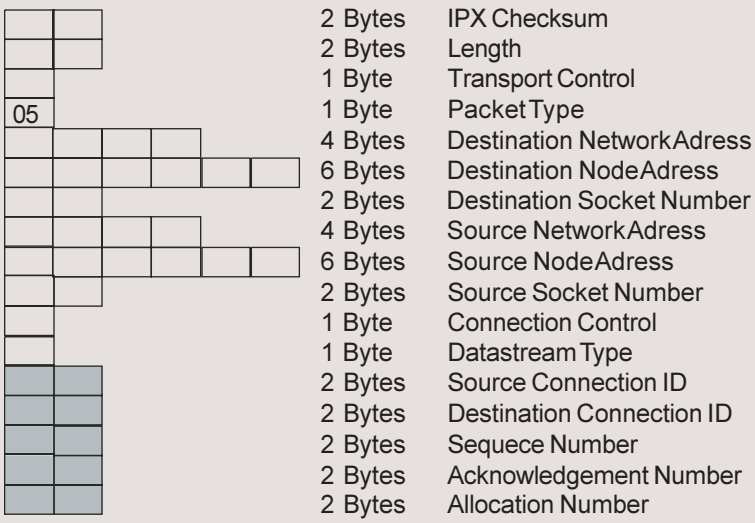

05
2 Bytes IPX Checksum
2 Bytes Length
1 Byte Transport Control
1 Byte Packet Type
4 Bytes Destination Network Adress
6 Bytes Destination Node Adress
2 Bytes Destination Socket Number
4 Bytes Source Network Adress
6 Bytes Source Node Adress
2 Bytes Source Socket Number
1 Byte Connection Control
1 Byte Datastream Type
2 Bytes Source Connection ID
2 Bytes Destination Connection ID
2 Bytes Sequece Number
2 Bytes Acknowledgement Number
2 Bytes Allocation Number

Abb. 4: Aufbau des SPX-Headers, wobei sich es beim vorderen Teil um den IPX-Header handelt.

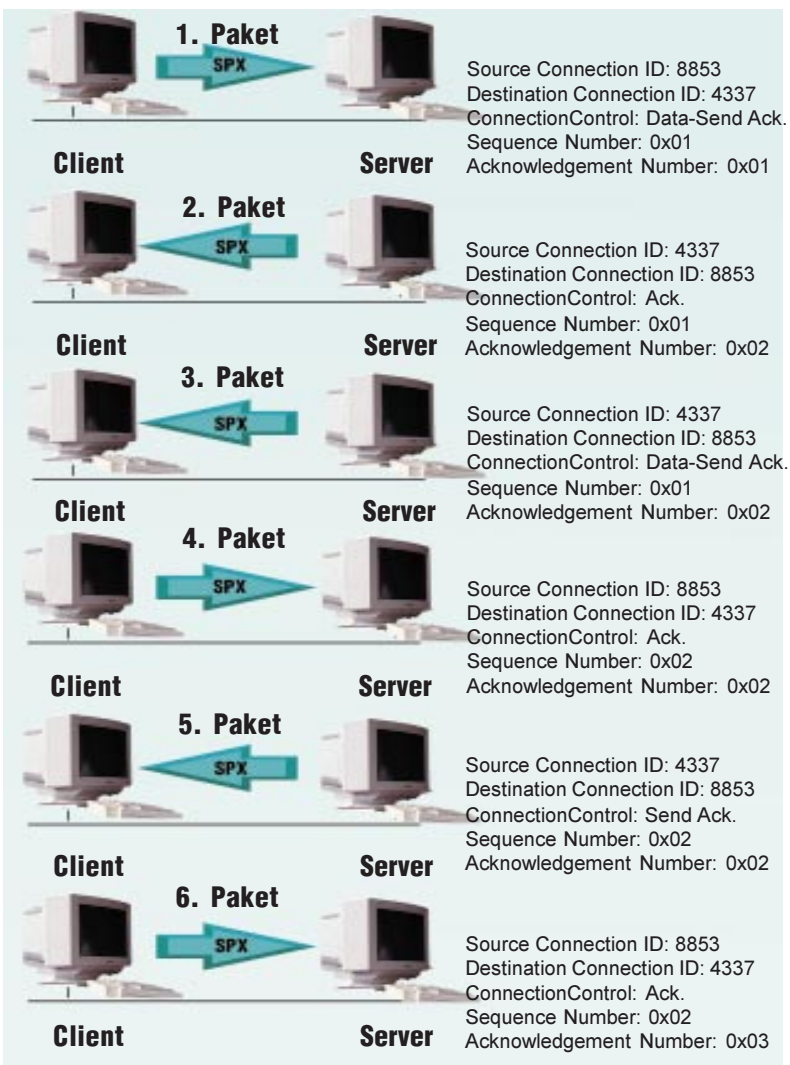


Abb. 5: Ablauf einer fehlerfreien Kommunikation anhand der Informationen Source Connection ID, der Destination Connection ID, des Connection Control Felds der Sequence Number und des Acknowledgement Number Feldes.

Dienstleister

In dem Bereich für die Anwendungen wird das Datastream Type Feld unter anderem für die Steuerung des Druckerdienstes von Novell genutzt. Der Wert `0x01` hält beispielsweise den Druckvorgang an und löscht den Pufferinhalt, wogegen der Wert `0x02` den Druckauftrag nur anhält, die Daten jedoch beibehält und auf weitere Anweisungen warten läßt.

Das zwei Byte lange Feld `Source Connection ID` wird vom Sender festgelegt und kennzeichnet durch seinen Wert die SPX-Verbindung. Durch diese eindeutige Kennzeichnung und Zuordnungsmöglichkeit können mehrere SPX-Verbindungen zur selben Zeit unterstützt werden.

Bei dem folgenden 2 Byte lange Feld `Destination Connection ID` handelt es sich um den Komplementär zum Feld `Source Connection ID`. Über die Destination Connection ID wird eine ID des SPX-Verbindungspartner vergeben. Beim ersten Paket ist dieser Wert immer auf `0xFFFF` festgelegt, da noch keine Festlegung durch den Verbindungspartner erfolgen konnte. Der Wert `0xFFFF` im Source Connection ID Feld eignet sich hervorragend, um Pakete für einen Verbindungsaufbau aus dem Datenstrom herauszufiltern.

Über das 2 Byte lange Feld `Sequence Number` wird die Anzahl der übertragenen Datenpakete einer Station angezeigt. Der Wert des Sequence Number Felds wird immer um eins erhöht, wenn eine Bestätigung des vorher übertragenen Datenpaketes empfangen wurde. Erreicht der Zähler den maximalen Wert von `0xFFFF`, so wird bei `0x0000` erneut begonnen und weitergezählt.

Für die Überwachung einer fehlerfreien Kommunikation wird das 2 Byte lange Feld `Acknowledgement Number` genutzt. Durch das Acknowledgement Number Feld wird die Sequenznummer des vom Verbindungspartner als nächstes erwartete SPX-Paketes angegeben. Stimmen diese Sequenznummern nicht überein, so geht die empfangende Station von einem verloren gegangenen Datenpaket aus. Das Feld

Allocation Number hat eine Länge von 2 Bytes und gibt die Anzahl der verfügbaren Empfangspuffer auf der Workstation-Seite an. Der Anfangswert liegt bei 0x00 und zeigt den ersten verfügbaren Empfangspuffer an. Der Wert 0x05 beispielsweise zeigt 6 verfügbare Empfangspuffer an, siehe Abb. 4.

Handshake

Vor dem eigentlichen Datenaustausch zwischen zwei Kommunikationspartnern auf der Basis des SPX-Protokolls muß erst eine SPX-Verbindung aufgebaut werden. Dabei wird ein Verfahren genutzt, was als Two-Way-Handshake bezeichnet wird. Dafür eröffnet beispielsweise ein Client einen Socket, in dem er an den Server eine Anforderung nach dem Motto: Meine Connection ID ist 34567, deine Connection ID ist 65535 verschickt. Der Server antwortet beispielsweise, meine Connection ID ist 23456 und deine Connection ID ist 34567. Innerhalb der folgenden Kommunikation zwischen den beiden Partnern werden diese beiden IDs genutzt, um die SPX-Verbindung eindeutig zu kennzeichnen.

Während des darauffolgenden Datentransfers startet der Client mit einer Anforderung, die die Sequence Number 0 und ebenfalls die Acknowledgement Number 0 beinhaltet. Darauf antwortet der Server mit einer Bestätigung, die ebenfalls die Sequence Number 0 und die Acknowledgement Number 1 beinhaltet. Mit dieser Antwort, welche die Acknowledgement Number 1 beinhaltet, wird zum einem die als nächstes erwartete Sequence Number der Gegenstelle angegeben und zum anderem die Anforderung bestätigt. Eine Bestätigung ist dabei immer die Basis für das Erhöhen der Sequence Number auf der Gegenseite. Die Sequence Number in den Paketen vom Server bleiben bei der Kommunikation solange auf 0, solange er keine eigenen Daten sendet. Dies ist jedoch bei einer typischen Kommunikation nicht immer der Fall und macht die Verfolgung des Datenaustauschs etwas komplizierter. Sendet der Server eigne Daten, so erhöht sich dessen Sequence Number ebenfalls, nachdem seine Daten bestätigt wurden (siehe Abb. 5).

Beendigung einer Verbindung

Für die Beendigung einer SPX-Verbindung wird eine End-Of-Connection-Anforderung an den Kommunikationspartner geschickt. Die SPX-Verbindung wird daraufhin beendet und die Gegenstelle antwortet nochmals mit einer End-of-Message-Bestätigung. Zum Austausch zusätzlicher Daten muß dann erst wieder eine neue SPX-Verbindung aufgebaut werden. Für die Protokollanalyse eines Datenaustauschs zwischen zwei Kommunikationspartnern sind die Inhalte des Source Connection ID Feldes, des Destination Connection ID Feldes, die Bits des Connection Control Feldes, die Sequence Number und das Acknowledgement-Feld innerhalb des SPX-Headers von Bedeutung. Anhand dieser Felder kann man eine fehlerfreie von einer fehlerhaften Kommunikation unterscheiden, siehe Abb. 5.

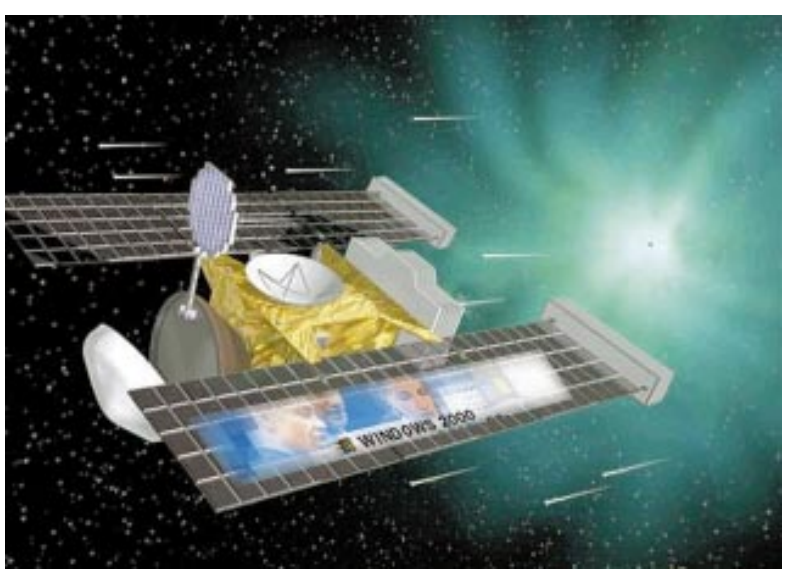
In der nächsten Ausgabe der Technik News wollen wir mit den Fehlerkontrollmechanismen, den Neuerungen durch SPX-II, dem NetWare-spezifischen Routing Protokoll und dem Service Advertising Protocol fortfahren.

MICROSOFT

2000 kommt

Letzte Beta-Phase für Windows 2000

Microsoft geht mit Windows 2000 Professional und Server Beta 3 in die letzte große Test-Phase vor der Produktverfügbarkeit und startet gleichzeitig mit dem Corporate Preview Programm (CPP). Ab Juni werden an deutsche Unternehmen rund 25.000 Versionen versandt.



Während die dritte Beta-Test von Windows 2000 primär dazu dient, das Produkt technisch intensiv zu testen, ermöglicht die Preview - beispielsweise den Support-Abteilungen von Unternehmen, Schulungszentren oder Vertriebspartnern - die Vorbereitung auf das fertige Produkt. Um dies zu gewährleisten, wird jedes Produkt des Preview Programms mit mehreren Lizenzen ausgeliefert. Die Vorbereitungsphase erlaubt Unternehmen, binnen relativ kurzer Zeit nach Produktverfügbarkeit auf die neue Version upzudaten.

Bestandteile des CPP

Das Corporate Preview Programm besteht aus den Produkten: Windows 2000 Professional und Windows 2000 Server Beta 3 sowie aus einer umfangreichen technischen Dokumentation und Migrationstools. Technischer Support ist für beide Versionen während drei Monate über Newsgroups gewährleistet. Das Corporate Preview Programm kostet DM 98,60 inklusive MwSt. und wird ab Juni ausgeliefert. Die Software ist 300 Tage lauffähig. Wer die Installationen beibehalten möchten, kann auf Windows 2000 updaten. Bestellmöglichkeit gibt es im Internet über: `http: //www.microsoft.com / germany / windows2000 /cpp.`

NEUE PRAXIS-SERIE

Operation 2000

Vorschau auf unsere neue Praxis Serie zum Windows Script Host

Von Olivier Plein

Windows 2000 naht. Der Windows Script Host ist jetzt schon als Version mit etwas eingeschränktem Funktionsumfang für NT4 verfügbar. Er soll unter Windows 2000 dem Administrator die Möglichkeit geben, unabhängig von den Desktop-Tools zu administrieren. Wer schon mal 1000 User angelegt hat, weiß, daß die GUIs für große Datenmengen unzureichend sind. Sinnvoll erscheint eine Scriptabarbeitung, gerade auch für wiederkehrende und selektive Arbeiten.

Stellen Sie sich vor, Sie haben 2000 User in einer verschachtelten Gruppenstruktur, und für die Mitglieder einer oder mehrerer Gruppen ändern sich die Home-Verzeichnisse. Na dann, viel Spaß. Mit WSH jedoch lassen sich diese Aufgaben nach Erstellung eines Scriptes automatisieren. Dabei kommen die Scriptsprachen Visual Basic für VBScript oder Java für JScript zum Einsatz. Ein wenig Programmiererfahrung erleichtert Ihnen dabei also den Einstieg.

Was liegt an ?

WSH ist mächtiger als man zunächst glaubt. Folgende Arbeiten lassen sich zumindest unter Windows 2000 realisieren:

- Auslesen sämtlicher User- und Gruppenrelationen zu Dokumentationszwecken mit Import in eine Excel-Datei.
- Verändern von Dateien (z.b. `Boot.ini`) auf allen erreichbaren Rechnern im Netzwerk
- Zugriff auf alle evtl. ODBC-Datenquellen, Oracle, SQL
- welche NIC mit welcher MAC- und welcher IP-Adresse ist im Einsatz.
- Auslesen, Verändern und Abgleich von statischen DHCP-Reservierungen
- Zugriff auf User-Informationen von Netware 3.x und 4.x mit dem neuen ADSI
- Zugriff auf LDAP-Informationen etwa wie in Exchange
- Zugriff auf die Metabase von IIS 4.0
- Zugriff auf die Registry

Mehr dazu im neuen Workshop „Operation 2000“ in der kommenden Technik News 7/99.

Unternehmenskommunikation

Teil V: Neuerungen in der Administration

Von Helmut Tibes

Auf dieser vorerst letzten Besichtigungstour werden wir uns mit den Veränderungen und Neuerungen auseinandersetzen, die Novell in GroupWise 5.5 verwirklicht hat, um uns Administratoren das Leben angenehmer zu machen. Wir konnten in den vorangegangenen Beiträgen feststellen, daß GroupWise in der neuen Version eine Fülle von Verbesserungen auf der Benutzerseite und bei der Installation bereithält, wie sieht es auf der administrativen Seite aus?

Wir wollen Ihnen zeigen, was sich beim Einrichten des Nachrichtenservers in der neuen Version 5.5 verändert hat. Dabei spielen die administrativen Aufgaben an einer Arbeitsstation im NWAdmin ebenso eine Rolle, wie das Verständnis der blauen Kontrollfenster der Agenten auf dem Server. Wie Sie vielleicht selbst schon erkannt haben, ist ein GroupWise 5.5 Server bereits nach der Installation als Basissystem ohne weitere Einstellungen voll funktionsfähig. Haben Sie allerdings eine komplexere Struktur zu verwirklichen oder möchten Sie z.B. den Zugang zu den Benutzerkonten rein über TCP/IP laufen lassen, dann brauchen Sie weitergehende Kenntnisse, wo entsprechende Arbeiten auszuführen sind. Wir möchten im folgenden eine Grundsatzanleitung geben, ein Vordringen in alle Details der administrativen Neuerungen in GroupWise 5.5 ist im Rahmen dieses Berichts zwar nicht möglich. Aber wir können einige ausgewählte Bereiche beleuchten.

Zugriffsrechte

Die Sicherheit in einem System ist von entscheidender Bedeutung, weil es darum geht, unberechtigte Zugriffe zu unterbinden, ohne den berechtigten Anwendern das Leben allzu schwer zu machen. In der Vergangenheit war es recht umständlich, den Benutzerzugriff im Modus `direkt` zu realisieren. Entweder Sie erteilten den Benutzern alle Verzeichnisrechte auf das Postamtverzeichnis und uneingeschränkte NDS Objekt-Rechte, oder Sie sahen sich mit einer unübersehbaren Anzahl von Einzeleinstellungen konfrontiert. Dies hat unter Group Wise 5.5 nun endlich ein Ende.

Rechtevergabe

Ganz gleich, ob Sie sich noch im Installationsprozeß befinden und alle bereits bestehenden NDS Benutzerobjekte mit exakt den notwendigen Rechten ausstatten wollen, oder ob Sie später in einem bereits arbeitenden GroupWise System bei der Erzeugung eines einzelnen Benutzerkontos die Rechte zuweisen möchten, bedarf es nur noch eines einzigen Tastendrucks, um diese Aufgabe auszuführen.

Dies ist ein besonders großer Vorteil, wenn Sie - aus welchen Gründen auch immer - einen Client/Server-Zugriff wieder in einen direkten Zugriff zurückführen möchten.

Auf das, was Sie zu tun haben, wenn Sie GroupWise 5.5 neu installieren, brauchen wir hier nicht einzugehen, denn der Dialog zur Festlegung der Benutzer-Systemrechte wird Ihnen

auf einem silbernen Tablett serviert. Wie Sie die Einstellungen nachträglich vornehmen, möchten wir Ihnen aber nicht vorenthalten. Es gibt prinzipiell zwei Möglichkeiten der Vorgehensweise.

Rechte zuweisen

Die erste ist die, daß Sie einem einzelnen Benutzer die Rechte zuweisen. Hierzu brauchen Sie nur im NWAdmin32 auf das NDS-Benutzerobjekt zu gehen, es mit einem Druck auf die linke Maustaste zu aktivieren und anschließend in der Menüleiste unter `Werkzeuge / GroupWise-Dienstprogramme / Rechte festlegen` zu wählen. In dem darauf folgenden Dialogfenster bestätigen Sie, daß die Systemrechte festgelegt werden sollen. Vermutlich erhalten Sie jetzt einen Hinweis, daß die Rechte erst festgelegt werden können, wenn das Postamt dafür vorbereitet wurde. Sie können das gleich an dieser Stelle nachholen oder auch auf das entsprechende Postamtobjekt in der NDS gehen und unter dem Tabulator Mitgliedschaft den Schalter `Zugriffsrechte festlegen` setzen (vgl. Abb. 1).

Rechte entfernen

Sollten Sie den zuletzt genannten Weg wählen, werden Sie eine interessante Feststellung machen. Es gibt einen weiteren Schalter dort, mit der Bezeichnung `Zugriffsrechte entfernen`. Sie sehen, es wird zum Kinderspiel von einem Zugriff über UNC-Pfad, sprich vom direkten Modus, zu einer TCP/IP-Verbindung, also zum Client/Server-Modus zu wechseln und umgekehrt. Wünschen Sie, daß alle neu angelegten GroupWise Benutzerkonten von Anfang an über die entsprechenden Rechte verfügen, dann können Sie das im NWAdmin32 unter `Werkzeuge/GroupWise-Systemoperationen/Einstellungen` in dem erscheinenden Dialog `Einstellungen für Admin` mit dem Marker `Zugriffsrechte automatisch festlegen` bestimmen. Zur Kontrolle, welche Zugriffsmethode eingestellt ist, können Sie im Kontrollfenster des POA (POstamt Agent) auf dem Server über die Funktionstaste `[F9]` die Log-Datei einsehen, denn hier werden alle Einstellungen festgehalten. Über `[ESC]` kann die Log-Datei wieder geschlossen werden. Beachten Sie aber, daß Änderungen erst um Mitternacht ihren Niederschlag finden, dann wird nämlich eine neue Log-Datei begonnen. Wollten Sie die Einstellungen unmittelbar sehen, müßte der Agent neu gestartet werden.

Benutzer-Synchronisation

Wie wir wissen, ist in GroupWise 5.5 einer der drei Agenten arbeitslos geworden. Die Rede ist vom ADA (ADministrations Agent), dessen Funktionalität teilweise in den POA (Post Office Agent) und teilweise in den MTA (Message Transfer Agent) eingeflossen ist. Für die NDS-Benutzer-Synchronisation ist jetzt der MTA verantwortlich, der diese Aufgabe mit einer deutlich verbesserten Bedienerführung wahrnimmt, was die Arbeit des Administrators sehr erleichtert. Bisher mußte umständlich ein Benutzerkonto eingerichtet werden, wenn wir kein Standardsystem vor uns hatten, um die Benutzer-Synchronisation sicherzustellen.

MTA konfigurieren

Der MTA kann von überall im System und für mehrere Domänen gleichzeitig die Synchronisationsaufgaben übernehmen. Die Rechte, die er hierzu braucht, und die Zuordnung zum System kann in einem Dialog und ohne zusätzliche Arbeiten vorgenommen werden. Die Zugriffssteuerung ist ebenso unproblematisch wie die vorhin besprochene Benutzer-Rechtevergabe und umfaßt einzig die Angabe des Servers, der das NetWare Loadable Module `MTA.NLM` ausführt. Und so wird es gemacht. Das Dialogfenster, mit dem Sie den MTA für den Abgleich mit der NDS einstellen können, erreichen Sie über `Werkzeuge/GroupWise-Systemoperationen/NDS-Benutzersynchronisierung`. Das Hauptfenster `Konfiguration der NDS-Benutzersynchronisierung` gibt Ihnen einen Überblick darüber, welche Domänen Ihr System umfaßt und ob diese einen Zugriff auf die NDS besitzen.

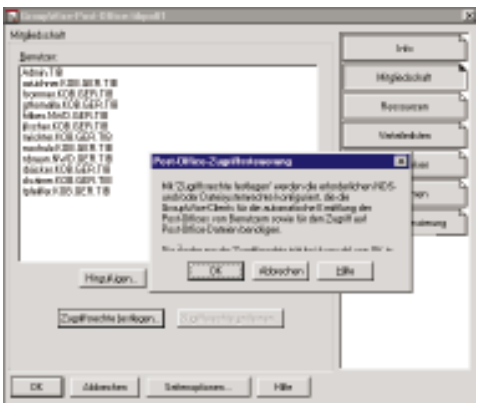


Abb. 1: Für das Postamt können die Objekt- und Dateirechte auch zentral auf dem Tabulator für die Mitgliedschaft vergeben werden.

NDS-Zugriff

In einem weiteren Feld sehen Sie den Agenten, der für die Synchronisation von GroupWise und NDS eingerichtet wurde (vgl. Abb. 2). Ist hier noch kein Eintrag vorhanden, müssen Sie durch Betätigen des Schalters `Agenten konfigurieren` erst einen MTA hierfür vorbereiten. Im folgenden Dialog wählen Sie einen Agenten aus – in der Regel ist dies jetzt ein MTA – und richten ihn für den Zugriff auf die NDS ein, indem Sie den gleichlautenden Schalter drükken. Sie brauchen jetzt nur noch zu dem NetWare Server zu browsen, auf dem der Agent ausgeführt wird und bestätigen die Eingabe zweimal mit `OK`. Wie im Fenster `Agenten konfigurieren` nun zu lesen ist, können wir hier erst fortfahren, wenn der Agent auf der Server Konsole über die Funktionstaste `[F6]` zu einem Neustart veranlaßt wurde. Ist dies geschehen und wird das Fenster durch Schließen und erneutes Öffnen aktualisiert, steht im Feld für den NDS Zugriff jetzt ein `Ja`. Ihre Aufgabe besteht nun darin, über den Schalter

aktivieren die NDS Benutzer-Synchronisation durch den Agenten zu starten und den Dialog über OK zu verlassen. Im Hauptfenster klicken Sie auf Zuordnung ändern, um im folgenden Fenster über den Schalter auswählen den Agenten zu bestimmen, welcher sich mit der Domäne synchronisieren soll. Automatisch gelangen Sie wieder zum ersten Dialog, der Ihnen jetzt die gerade getätigte Konfiguration darstellt, siehe Abb. 2. Über OK und Schließen beenden sie den Vorgang. Auch hier gilt, was bereits zum POA gesagt wurde. Die Konfiguration wird in der Log-Datei festgehalten und kann dort unter NDS Erkennung und NDS-Benutzersynchronisation eingesehen werden. Ein Neustart des MTA ist über die Funktionstaste [F6] möglich.

Konvertierung externer Einheiten

Kennen Sie das Problem nicht auch? Sie haben Außendienstmitarbeiter, die nur über ein GroupWise Konto verfügen, aber innerhalb der NDS nicht als Benutzer geführt werden. Jetzt kommt dieser Mitarbeiter in den Innendienst und erhält auch ein NDS-Benutzerkonto. Wie aber das E-Mail-Konto und den NetWare Account zusammenbringen? Wir wollen doch nicht zwei Objekte mit Arbeitsteilung in unserer NDS haben.

Unter 5.2

Sollten Sie in GroupWise 5.2 einmal vor einem solchen Problem gestanden haben, werden Sie sich sicher erinnern, wie umständlich der Workaround hierfür aussah, denn es gab keine "offizielle" Möglichkeit. Sie mußten zuerst mit einem NWAdmin arbeiten, der nicht über die GroupWise SnapIns – das sind Dateien für die Darstellungserweiterungen durch GroupWise – verfügte. Sie löschten daraufhin das Objekt Externe Einheit in der NDS, welches ja als Fragezeichen erschien. Sinn dieser Geschichte war es, das NDS-Objekt, nicht aber das GroupWise-Konto zu löschen. Für die Fortführung der Aufgabe bedienten Sie sich jetzt eines NWAdmins mit SnapIns und legten einen NDS-Benutzer an, welchem Sie die GroupWise ID der gelöschten Externe Einheit gaben. Sie bestätigten noch, daß Sie NDS-Objekt und GroupWise-Konto aneinander binden wollten, und hatten so aus einer Externen Einheit ohne NDS-Konto ein NDS-Konto mit GroupWise-Konto gemacht, ohne die E-Mails zu verlieren. Dennoch sehr umständlich, finden Sie nicht auch?

Unter 5.5

Mit GroupWise 5.5 ist dies alles nun eine Sache von Sekunden und bedarf nur weniger Einzelschritte, wie Sie jetzt sehen werden. Dazu gehen Sie mit der Maus auf das NDS-Objekt Externe Einheit und aktivieren es mit der linken Maustaste, so daß das Objektbild blau hinterlegt ist. Anschließend unter Werkzeuge/GroupWise-Dienstprogramme/Externe Einheit konvertieren anwählen (vgl. Abb. 3) und die Frage Konvertierung durchführen durch Klick auf die Taste JA bestätigen und mit OK die Konvertierung abschließen. Damit Sie das Ergebnis sehen können, müssen Sie nur den Behälter des Objektes einmal schließen und wieder öffnen, und Sie werden feststellen, daß unsere Externe Einheit zu einem vollwertigen Mitglied unserer NDS geworden ist. Wie gewöhnlich können Sie die Information über die Änderung des Objektes auch im Protokollfenster des Kontrollschirms des POA auf dem Server verfolgen. Sie müssen wissen, daß auch die administrativen Befehle in Form von E-Mails an die ausführende Komponente in GroupWise weitergeleitet werden (siehe Abb. 3).

TCP/IP-Postamtverbindungen

Vielleicht hatten Sie schon einmal mit einem größeren GroupWise 5.2 System zu tun. Dann waren Sie sicher auch schon einmal mit der Schwierigkeit konfrontiert, eine Verbindung zu Außenstellen herzustellen. Die Frage war wohl, wie die Mitarbeiterinnen und Mitarbeiter an einem anderen Standort an die entfernte GroupWise Domäne angebunden werden sollen. Es war schon ein tiefergehendes Verständnis der Arbeitsweise notwendig um zu wissen, wie GroupWise den Nachrichtentransport organisiert. Sie fanden dann heraus, daß neben dem Postamt vor Ort und damit dem Postamt-Agenten auch ein Message Transfer Agent notwendig war. Dieser nahm die Nachrichten, welche der lokale Benutzer einem entlegenen Empfänger zusenden wollte, vom POA entgegen und leitete sie an den MTA der Domäne weiter, der wiederum den MTA des anderen entlegenen Standorts ansprach. Sie stellten fest, daß an jedem Ort, an welchem Sie ein Postamt betreiben wollten, ein MTA erforderlich war. Obendrein war für die NDS Synchronisation auch noch an jeder Außenstellen eine ADA zu konfigurieren.

Post Office Agent

Das alles hat sich mit der neuen GroupWise Version gewaltig geändert, mit dem Vorteil eines deutlich verringerten administrativen Aufwands und erheblich reduzierter Konfigurationsarbeit. Sie brauchen jetzt je Standort nur noch einen einzigen Agenten. Der Postamt-Agent übernimmt nun sämtliche Aufgaben, seine eigenen, eben die der Verbindungsherstellung zum Benutzer, ebenso wie die des MTA, also die Herstellung des Links zum Domänen-MTA (vgl. Abb. 4). Sie könnten jetzt sagen, daß das sehr gefährlich ist in Bezug auf die Betriebssicherheit des Systems, aber diese Bedenken kann ich problemlos zerstreuen. Die Agenten haben auch bisher schon mit sogenannten Prozessen gearbeitet. Sollte ein Prozeß gestört sein, wurde der betroffene Ablauf angehalten, ohne die restlichen Aufgaben zu beeinträchtigen. Jetzt sind einfach nur alle Prozesse unter einem Dach, besser unter einem Namen zusammengefaßt, aber sie funktionieren wie bisher. Ist also nur eine Funktion betroffen, und

legt diese Funktion nicht gleich den ganzen Server lahm, geht der Rest seiner gewohnten Arbeit nach. Sie haben also etwas Luft bei der Fehlerbeseitigung.

Mitteilungs-Transport-Prozeß

Der Prozeß, den der POA vom MTA übernommen hat, heißt MTP oder Mitteilungs-Transport-Prozeß und regelt die Verbindungsherstellung zur Domäne und den Nachrichtenaustausch mit dem ihr unterstellten MTA. Aber was haben Sie jetzt zu tun, um die Kommunikation der Postämter untereinander sicherzustellen? Ganz einfach, nur zwei Kleinigkeiten sind auf dem Weg zu einer erfolgreichen Verbindung zu erledigen. Zu allererst müssen dem System Adressen mitgeteilt werden. In unserem Fall handelt es sich um die IP-Adresse des Servers, auf dem der POA betrieben wird, und den Port, an dem der POA auf die Nachrichtenlieferung wartet.

IP-Adresse und Port

Wir können das gleich einmal praktizieren, indem wir den NWAdmin32 starten, uns das Objekt des außenliegenden Postamts im NDS-Baum suchen und den dort beheimateten POA doppelklicken. Mit der linken Maustaste wechseln wir auf den Tabulator `Netzwerkadresse` und sehen sofort das neue Feld `Nachrichtentransportanschluß`, welches aber noch nicht aktiv ist. Damit sich das ändert, müssen wir zuerst die TCP/IP-Adresse eintragen. Hierzu setzten wir unter `Nachrichtenprotokoll hinzufügen` einen Marker neben `TCP/IP` und drücken anschließend den Schalter `Hinzufügen`, der jetzt verfügbar wird. Es erscheint nun der Dialog `Netzwerkadresse hinzufügen`, der es uns ermöglicht, neben der Bezeichnung IP die Server-Adresse zu hinterlegen. Der untenstehende `Port 1677` ist der Standard Port für den Client/Server-Zugriff und soll uns an dieser Stelle nicht beschäftigen. Mit `OK` wird der Eintrag übernommen und nach dem Rücksprung in das Agentenfenster kann jetzt der Port – standardmäßig `7100` – in das Textfeld geschrieben und mittels `OK` übernommen werden (vgl. Abb. 5).

Link konfigurieren

Der zweite Schritt besteht darin, den Link zu konfigurieren. Dies wird ebenfalls im NWAdmin32 ausgeführt und zwar unter `Werkzeuge/GroupWise-Dienstprogramme/Verbindungskonfiguration`. In dem erscheinenden Programmfenster wählen Sie `Anzeigen/Post-Office-Verbindungen` und gehen dann mit dem Mauszeiger auf die Verbindung, die Sie auf TCP/IP einrichten wollen. Rechte Maustaste/bearbeiten und als Protokoll `TCP/IP` einstellen und `OK`. Schließen Sie jetzt das Programmfenster und bestätigen Sie, daß Sie die

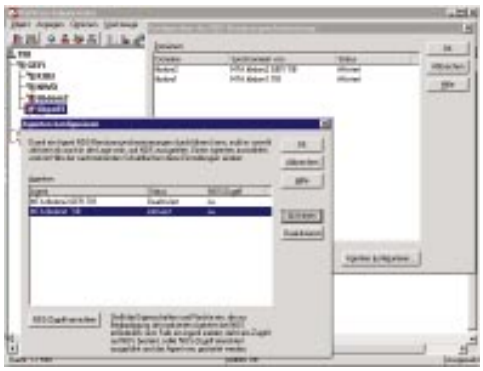


Abb. 2: Mit der GroupWise Systemoperation "NDS-Benutzersynchronisation" kann ein MTA für den Abgleich mit der NDS konfiguriert werden

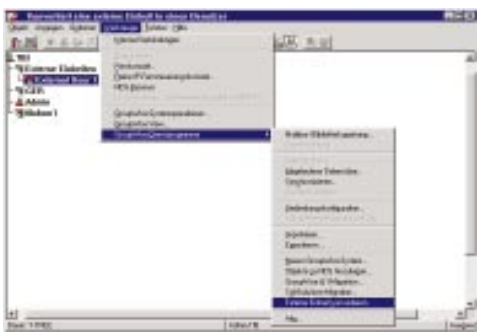


Abb. 3: Externe Einheiten können in GroupWise 5.5 in einem einzigen Arbeitsgang zu einem NDS Objekt konvertiert werden.

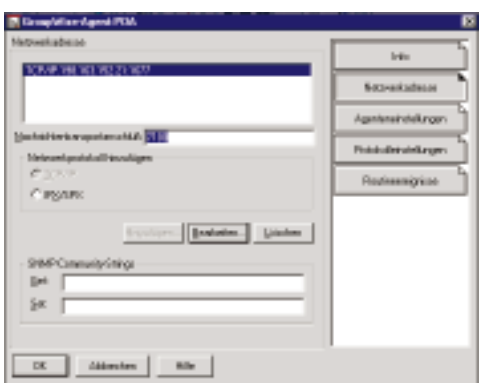
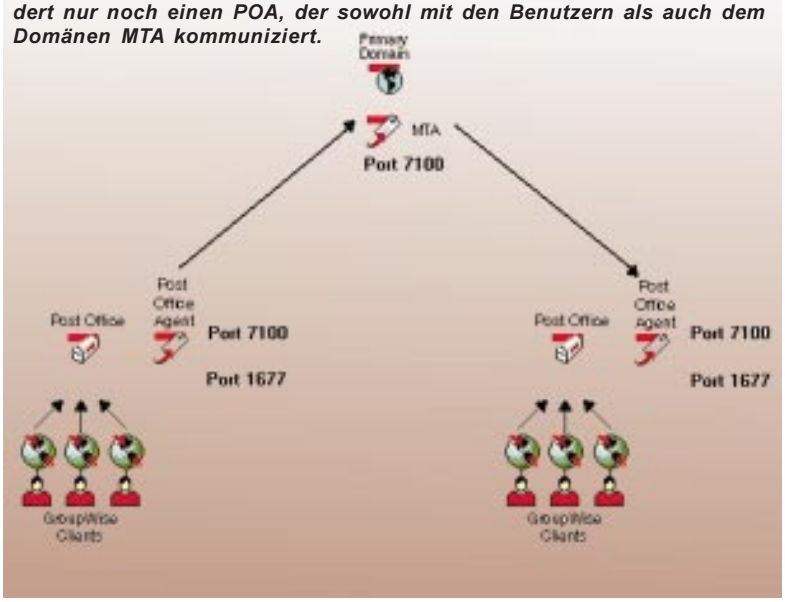


Abb. 5: In GroupWise 5.5 übernimmt der ausgelagerte POA die Funktion des MTA bei dem Postamt-übergreifenden Nachrichtentransport.

Abb. 4: Die Konfiguration eines Systems mit ausgelagertem Postamt erfordert nur noch einen POA, der sowohl mit den Benutzern als auch dem Domänen MTA kommuniziert.



Änderungen speichern wollen. Damit sind alle notwendigen Einstellungen durchgeführt worden und Ihr Postamt startet beim nächsten Mal eine Kommunikation zur Domäne über TCP/IP.

Prüfung über tcpcon

Sie können prüfen, ob der POA die TCP/IP-Verbindung ordnungsgemäß aufbaut. Hierzu stehen mehrere Mittel zur Verfügung. Entweder Sie starten ein Modul zur Kontrolle der TCP-Verbindungen auf dem Server, indem Sie auf der Konsole `load tcpcon` eingeben. Dann wechseln Sie unter `Available Options` zu `Protocol Information / TCP / TCP Connections`, damit Sie durch Drücken der Taste `ENTER` und Auswählen durch die Pfeiltaste unten/oben die entsprechende TCP-Verbindung anschauen können. Wichtig ist, daß der `Port 7100` aufgeführt wird und der dazugehörige Status `Listen` also auf `Empfang` steht.

Prüfung über POA

Die andere Möglichkeit, das Zustandekommen eines Links zu kontrollieren, ist, auf dem Server zum Agenten-Fenster des POA zu wechseln und über die Funktionstaste `[F10]` die Options-Liste aufzurufen. Position 5 ist die Auswahl `Message Transfer Status` und liefert uns folgende Informationen. Die `Outbound`- und `Inbound`-Einträge zeigen die IP-Adressen des MTA auf dem Server mit dem GroupWise System und die IP-Adresse des eigenen Servers, auf dem nur das Postamt läuft. Wichtig ist noch das mittlere Feld, hier können der aktuelle Status `open` oder `closed` gesehen werden. Eine Historie gibt die Zeiten der letzten Öffnung und Schließung an und zeigt den Grund der letzten Schließung. Der Link sollte grundsätzlich geöffnet sein, kann aber hin und wieder auch einen geschlossenen Zustand annehmen.

POA-Startschalter

Die Startup-Datei des POA weist einige neue Schalter auf, welche die Funktionalität des Postamt-Agenten erweitern. Diese Schalter sind in der Regel nicht gelegt und müssen bei der Konfiguration im Startup-File aktiviert werden. Eine Ausnahme hierbei macht die `nächtliche Benutzerwartung`, die über zwei Schalter verfügt. Mit dem ersten `/nonuu` (no nightly user upkeep) kann die Benutzerwartung abgeschaltet werden und der zweite `/nuuoffset-1` (nightly user upkeep offset) legt die Stundenzahl fest, mit der die Benutzerwartung auf eine Zeit nach Mitternacht verschoben wird (vgl. Abb. 6).

Nächtliche Benutzerwartung

Wird die Verzögerung eingeschaltet, ist standardmäßig die Benutzerwartung für 1 Uhr Nachts angesetzt. Der Vorteil der nächtlichen Benutzerwartung liegt ganz klar auf der Seite des Benutzers, denn die Benutzerwartung läßt bestimmte Aufgaben während der Nacht durch den POA automatisiert ablaufen. Dadurch werden z.B. das Entfernen abgelaufener Dateien aus dem Papierkorb, das Löschen abgelaufener Nachrichten aus der Mailbox oder der Abgleich des Adreßbuches für häufige Kontakte mit dem Systemadreßbuch nicht mehr während der Benutzung des Clients tagsüber durchgeführt. Die Folge ist eine deutlich schnellere Benutzeroberfläche, die nicht plötzlich das Arbeiten einstellt, weil die o.a. Aufgaben erledigt werden müssen.

Startup-Datei

Übrigens, wir hatten vergessen, Ihnen zu sagen, daß Sie die Startup-Datei auf dem Volume `SYS` im Systemverzeichnis finden und die Datei den Namen Ihres Postamtes trägt, also `postamtname.poa`. Einen weiteren, sehr nützlichen Schalter finden Sie ebenfalls in dieser Datei. Er trägt die Bezeichnung `/rights` und führt dazu, wenn er gesetzt wird, daß der POA, ehe er das Postamt startet, erst einmal die gesamte Verzeichnisstruktur auf die Zugriffsrechte hin überprüft. Dabei werden auch auf andere Server ausgelagerte Verzeichnisse mit in die Prüfung einbezogen. Alle Informationen können während des Starts des POA im Agenten-Fenster auf dem Server mitgelesen werden. Gibt es keine Beanstandungen, ist sichergestellt, daß der POA, was den Dateizugriff anbelangt, einwandfrei arbeiten wird. Dieser Schalter ist also für Tests beim erstmaligen Starten oder bei der Fehlersuche ein nützliches Hilfsmittel. Schließlich wurde ein dritter Schalter dem Startprofil zugefügt, der das Login auf einem entfernten Server wesentlich erleichtert. Bisher mußte der POA mit einem Benutzereintrag und einem Paßwort versorgt werden, damit er sich auf einem Remote-Server anmelden konnte. Dies machte es sehr oft erforderlich, in der NDS ein zusätzliches Benutzerkonto anzulegen. Mit GroupWise 5.5 gehört dies der Vergangenheit an. Jetzt muß nur noch der Schalter `/dn` (distinguished name) gelegt werden und der POA ist nach dem nächsten Neustart in der Lage, sich auf dem Remote-Server anzumelden. Nebenbei soll nur erwähnt werden, daß der MTA ebenfalls über einen solchen Schalter verfügt.

WAN-Verbindungsplanung

Ein großes Problem in der Vergangenheit war, mehrere Domänen über eine WAN-Strecke miteinander zu verbinden. War zwischen den Systemen aufgrund des Nachrichtenaufkommens eine Standleitung nicht zu rechtfertigen und trat an ihre Stelle eine Wählleitung, hatte man kaum Möglichkeiten, den Verkehr auf der WAN-Strekke zu planen. Die Verbindungsplanung unter GroupWise 5.5 gibt dem Administrator hier ganz neue Möglichkeiten an die Hand. Wir wollen uns das einmal anschauen.

Streckenplanung

Wie gewöhnlich werden diese Aufgaben im NWAdmin32 umgesetzt. Hierzu gehen Sie wieder in die Oberfläche für die Verbindungskonfiguration und wählen die entsprechende Domäne, von welcher der Verbindungsaufbau gestartet werden soll, aus. Sie

stellen also z.B. die Primärdomäne in der Auswahlliste ein und führen einen Doppelklick auf dem Eintrag unter Ausgangsverbindung von Primärdomänenname aus. Der nun geöffnete Dialog liefert Ihnen einen Schalter Planung, den Sie bitte betätigen. Jetzt haben Sie die Möglichkeit, ein Verbindungsprofil zu erstellen, welches sich vollständig an Ihren Bedürfnissen orientiert.

Domänenverbindung

Neben der absoluten Zeitsteuerung, die Ihnen in Form eines Wochenkalenders mit halbstündiger Unterteilung präsentiert wird, können Sie das Öffnen der Domänenverbindung sogar differenziert bis auf die einzelnen Warteschlangen herunterbrechen (vgl. Abb. 7). Sie haben also die Möglichkeit, zwischen Benutzernachrichten hoher, mittlerer und niedriger Priorität, den administrativen Nachrichten und den Anfragen der Remote-Benutzer zu unterscheiden. Außerdem können Sie den Verkehr, der durch die Suche nach freien Terminzeiten oder die Statusinformationen zustande kommt, auf diese Weise steuern. Nicht zuletzt läßt sich die Verbindung auch kontrolliert über die Anzahl der Nachrichten oder ihren Platzbedarf in Kilo Byte aufbauen. In diesem Zusammenhang soll nicht unerwähnt bleiben, daß der MTA ab GroupWise 5.5 keinen Unterschied mehr zwischen TCP/IP und kopierten Dateien (UNC-Pfad) macht. Es gibt also keine unterschiedlichen Transportrouten mehr, sondern alle Nachrichten werden grundsätzlich durch das Verzeichnis MSLOCAL/GWINPROG geleitet.

Weitere Neuerungen

Die Version 5.5 verfügt jetzt über eine Funktion für AUTO-CONNECTING. Immer wenn Sie versuchen, GroupWise-Objekte zu verändern, die nicht zu dem System gehören, mit dem Sie momentan verbunden sind, wird Ihnen automatisch die Möglichkeit gegeben, sich im anderen System anzumelden. Ja, Sie können sogar GroupWise-Objekte in der NDS löschen, über OBJECT DELETION, selbst wenn Sie überhaupt nicht mit dem System verbunden sind.

Internet-Adressierung

Eine weitere Besonderheit in GroupWise 5.5 ist das INTERNET ADDRESSING. Es erlaubt Ihnen, GroupWise so einzustellen, daß Sie die Adressierung für interne wie für externe (Internet-) Benutzer gleich gestalten, eben im Internet-Format. Es werden aber weitere Adressierungs-Formate angeboten, was Ihr System sehr flexibel macht.
Außerdem unterstützt die neue Version MULTIPEL INTERNET DOMAIN NAMES. Das bedeutet, daß Sie Ihr Unternehmen nach außen hin über verschiedene Namen erreichbar machen können.
Sie sind sogar in der Lage, bis auf die Ebene der Benutzerebene hinab die Zuordnung zu den verschiedenen Domänennamen zu organisieren.

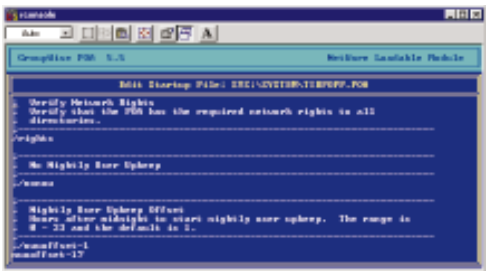


Abb. 6: Zusätzliche Schalter in der Startup-Datei des POA erweitern die Funktionalität und erhöhen den Komfort.

Abb. 7: Die Steuerung des Verbindungsaufbaus zwischen zwei über WAN-Strecke verbundene Domänen ist in Abhängigkeit der Zeit, der Nachrichtenanzahl und des Speicherbedarfs möglich.

Technik News Service-CD 2/99

Halbjährliche Extra-CD mit Standardpatches ab Juli fest im Abo

Die neue Service-CD 2/99 kommt im Juli heraus. Sie geht ab sofort an alle Technik News Leser. Sie enthält Patches und Updates zu den Produkten von Novell, Microsoft, AVM, Tobit, Bintec und jetzt auch zu Computer Associates (früher Cheyenne). NetWare 5 Patches und Service Packs werden erstmalig enthalten sein und auch die aktuellen Novell Clients.

Sommer-Trainings-Camp ´99

Durchstarten und Wohlfühlen mit Netzwerk-Seminaren bei Compu-Shack

Der Sommer steht vor der Tür. Da hat die Compu-Shack Education bekanntlich wieder viel für kühle Köpfe zu bieten, die in den heißen Tagen im Bereich der Netzwerktechnologien weiter nach oben wollen. So wendet sich auch in diesem Jahr das Compu-Shack "Sommer-Trainings-Camp ´99" wieder an alle Wissensdurstigen, die preisbewußt und hochmotiviert ihre Ausbildungsziele verfolgen möchten. Ein Angebot für alle, die bei einer Zertifizierung zum MCSE oder CNE die Vorteile eines kompetenten Schulungspartners schätzen und die Sommersonderpreise zu nutzen wissen.

Insider kennen noch das Anti-Sommerhitze-Programm der Compu-Shack Education als eine Institution, die in der schönsten Zeit des Jahres mit besonderen Angeboten aufwartet. Mit einem neuen Gesicht und interessanten Highlights für Schulungshungrige und Wissensdurstige präsentiert sich das "Sommer-Trainings-Camp ´99" in diesem Jahr noch attraktiver als zuvor. Aus ihrem aktuellen Kursangebot bietet die Compu-Shack Education 10% Bonus für ein Einzelseminar nach Wahl. Bei einer Komplettzertifizierung innerhalb einer CNE- oder MCSE-Ausbildung können Sie sogar bis zu 15% einsparen. Eine richtig heiße Sache wird das Sommer-Trainings-Camp nach jeder 10. Anmeldung, weil dann ein Seminar kostenlos zur Wahl steht! Kühle Rechner kommen in jedem Fall auf ihre Kosten.

Begehrt im Unternehmen

Warum nicht zuerst die beruflichen Träume verwirklichen und sich dann am Traumstrand erholen? In den voll klimatisierten Räumen der Compu-Shack Education, die technisch hervorragend ausgestattet sind, genießen die Teilnehmer selbst im heißesten Sommer eine streßfreie Ausbildung, die hohen Ansprüchen gerecht wird. Beispielsweise zum Microsoft Certified Professional. Der MCP besitzt praktisches und theoretisches Wissen über ein ausgewähltes Microsoft Produkt und ist aufgrund seiner Ausbildung in der Wirtschaft ein gefragter Mitarbeiter. Die Tests hierzu sind sehr anspruchsvoll und bedürfen einer intensiven Vorbereitung, weil sie produktspezifisch konzipiert werden. Und Netzwerkadministratoren dient der MCP als Grundlage zum Microsoft Certified Systems Engineer (MCSE), der insgesamt sechs Examen absolvieren muß: vier Betriebssystem-Prüfungen und zwei Tests aus den Wahlbereichen Microsoft Connectivity oder BackOffice.

Diplome geben Sicherheit

Parallel zu den Microsoft-Zertifizierungen kann man sich auch zum Certified Novell Administrator (CNA) qualifizieren. Mit den entsprechenden Vorbereitungskursen wie der Intranet-Ware Administration bietet Compu-Shack den richtigen Einstieg in ein begehrtes Berufsfeld. Aufbauend kann die Prüfung zum Certified Novell Engineer (CNE) absolviert werden, die den Techniker oder Ingenieur befähigt, ein Novell-Netzwerk professionell zu administrieren und implementieren.

Chancen wahren, Karrieren sichern

MCPs, MCSEs, CNAs und CNEs sind bestens qualifizierte Fachleute, die derzeit stark gesucht werden, und im IT-Bereich optimal eingesetzt werden können. Insoweit läßt sich das Sommer-Trainings-Camp in besonderem Maße zur beruflichen Qualifizierung nutzen. Denn diese zertifizierten Fachleute gewähren in einem entscheidenden Maße die Leistungs- und Konkurrenzfähigkeit eines Unternehmens. So dient ein Weiterbildungs- oder Zertifizierungsprogramm auch der persönlichen Sicherung des Arbeitsplatzes und erhöht die Chancen auf dem Arbeitsmarkt. Einer beruflichen Karriere stehen alle Türen offen. Die Compu-Shack Education berät gerne über das aktuelle Ausbildungsprogramm. Ein erfahrenes Team steht bereit, in Ruhe und ganz individuell den Wissensbedarf der Interessenten zu ermitteln und ein geeignetes Trainingsangebot zu erstellen.

CS Education-Hotline Neuwied/ München:

Dorothee Michels und Sonja Schlosser
Telefon: 02631 / 983-317
eMail: education@compu-shack.com

Wissensvorsprung

Compu-Shack Bookstore

Ganz gleich ob man sich auf die Zertifizierung zum Microsoft Certified Systems Engineer (MCSE) oder den Certified Novell Engineer (CNE) vorbereitet, oder einfach nur auf der Suche nach einer umfassenden Informationsquelle ist, Compu-Shack ist die richtige Adresse, wenn es darum geht, sich privat mit adäquater Fachliteratur weiterzubilden.

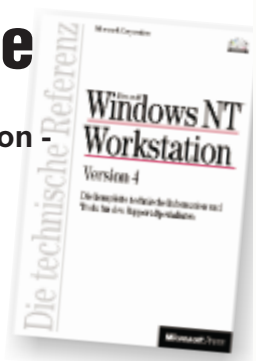
Die Compu-Shack Education bringt zukünftig original Trainings- und Schulungsunterlagen sowie begleitendes Material heraus. Es beruht auf den Unterlagen der Hersteller und wurde von Produktentwicklern, Support-Ingenieuren und Kursleitern erarbeitet. Diese professionellen Pakete für das Selbststudium verschaffen den notwendigen Wissensvorsprung. Sie überzeugen durch klar gegliederte Lektionen und direkten Praxisbezug.

Von Praktikern für Praktiker

Der technisch Interessierte erfährt alles über die Installation, die Konfiguration und den Support von Betriebssystem-Software und Netzwerken, von Microsoft- und Novell-Produkten sowie deren Integration und Administrierung. Ob für die modernen Betriebssysteme oder die Backoffice Software, fast zu jedem Thema gibt es Original-Student-Kits und Bücher der Microsoft- und Novell-Press sowie von O'reilly. Dabei spielt es keine Rolle, wie ehrgeizig das individuelle Lernziel gesetzt ist. Zur grundsätzlichen Informationen, zur Vorbereitung auf bestimmte Prüfungen oder nur für den Arbeitsalltag findet sich die passende Literatur im Bookstore der Compu-Shack Education.

auf der Bestellkarte können Sie den Bücherkatalog kostenlos anfordern

Bookstore



Microsoft Windows NT 4 Workstation - Die technische Referenz.

Microsoft Corporation,
1.400 Seiten mit 1 CD 98,- DM.
Microsoft Press: Dezember 1996.
ISBN 3-86063-240-X

Dieses exklusive Nachschlagewerk von Microsoft wurde in enger Zusammenarbeit mit den Entwicklungs- und Support-Abteilungen von Microsoft Windows NT Workstation verfaßt. Es stellt die vollständigste Quelle für technische Information dar und enthält grundlegende Referenzinformationen zur Installation, Konfiguration und Fehlerbehebung von Microsoft Windows NT Workstation Version 4.0. Zusätzlich bietet die beiliegende Begleit-CD (US-amerikanische Originalversion) mehr als 100 zusätzliche Dienstprogramme, die helfen, Microsoft Windows NT Workstation Version 4.0 noch effizienter einzusetzen bzw. zu unterstützen. Für Administratoren ist ein umfangreicher Abschnitt über die Einsatzplanung in Großunternehmen und die Kompatibilität zu vorhandenen Netzwerk- und Betriebssystemumgebungen enthalten.

Seminargruppen Übersicht

	Netzwerk Grundlagen
CS	Strukturierte Verkabelung
MS 578	Networking Essentials
NV 565a	Networking Technologies Entry Level
NV 565	Networking Technologies „Professional"
	Microsoft Windows 98
MS 954	Upgrading to Microsoft Windows 98
MS 955	Supporting Microsoft Windows 98
	Microsoft Windows NT 4.0
MS 685	Installing & Configuring WinNT Server 4.0
MS 689	Supporting MS WinNT 4.0 - Enterprise Technologies
MS 770	Installing & Configuring MS WinNT Workstation 4.0
MS 803	Administering Microsoft Windows NT 4.0
MS 922	Supporting MS WinNT 4.0 Core Technologies
MS 983	Accelerated Training Microsoft Windows NT 4.0
	Microsoft Windows NT 5/ Windows 2000
MS 1100	Upgrading MS WinNT 5.0
MS 1202	Securing MS Windows NT-Server
MS 1265	Installing & Administering MS Windows NT 5.0
MS 1266	Supporting Microsoft Windows NT 5.0
MS 1267	Planning & Implementing the Active Directory
	Microsoft Back Office
MS 828	Supporting MS Systems Management Server 2.0
MS 832	System Administration for SQL Server 7.0
MS 833	Implementing a Database in SQL Server 7.0
MS 932	Installing & Configuring Microsoft SMS Server 1.2
MS 958	Supporting Microsoft Cluster Server
MS 960	Supporting Routing & Remote Access Service for Win NT 4
MS 973	MS Exchange Server 5.5 Series -Design & Impl.
MS 981	Supporting Microsoft SNA Server 4.0
MS 1026	MS Exchange Server 5.5 Series -Concepts and Admin.
MS 1198	Microsoft Windows Terminal Server
	Novell Netware 4.11
NV 520	IntranetWare: NW 4.11 Administration
NV 525	IntranetWare: NW 4.11 Advanced Administration
NV 526	IntranetWare: NW 3 to 4.11 Update
NV 804	IntranetWare: NW 4.11 Installing & Configuring (Workshop)
	Novell NetWare 5.0
CS-WS	NetWare 5.0 Extreme Workshop
NV 529	NetWare 5.0 Update
NV 555	NetWare: Integrating WinNT Workstation & Server
NV 560	NetWare 5.0 Administration
NV 570	NetWare 5 Advanced Administration
NV 575	NDS Design & Implementation with NDS Workshop
NV 580	NetWare Service & Support
NV 780a	Z.E.N. Works – "Professional" !
NV 780	Z.E.N. Works - New Release !
	Novell Backoffice
NV 350	GroupWise 5 Administration
NV 352	GroupWise 5 Advanced Administration
NV 354	GroupWise Net Access and Connectivity
NV 720	NetWare for SAA Inst. & Troubleshooting
NV 730	Network Management with ManageWise 2.6
	Internet Seminare
MS 688	Internetworking mit Microsoft TCP/IP on NT 4.0
MS 836	Secure Web Access using Proxy Server 2.0
MS 857	Admininistering & Supporting Microsoft FrontPage 97
MS 936	Creating & Managing a Web Server using IIS 4.0
NV 605	NetWare TCP/IP Transport
NV 660	Designing Effective Web Sites
NV 770	Securing Intranets with BorderManager 3.0
	Fehlertolerante Systeme
MS 958	Supporting Microsoft Cluster Server
Vinca	VINCA StandbyServer für intranetWare 4.11
Vinca	VINCA StandbyServer für NetWare 5.0
Vinca	VINCA Co-StandbyServer für Windows NT
	Connectivity & Communications
Ascend	Configuring and Installing Ascend Max
AVM	ISDN MultiProtocol Router for Windows NT 1.x
AVM	NetWare Connect for ISDN 2.x
AVM	NetWare MultiProtocol Router for ISDN 3.x (AVM)
AVM	NetWork Distributed ISDN 1.x
Bintec	Bintec Basic Entry
Bintec	Bintec Professional Configuring
Citrix	Citrix WinFrame Enterprise
Cisco	Cisco Vorbereitung
Cisco	Cisco Essentials Small & Medium Business
Cisco	Cisco Designing Networks
Cisco	Introducing Cisco Router Configuration
Cisco	Cisco Router & LAN Switch Configuration

Novell CDs

Kostenlose Trials und Datenblätter auf der Compu-Shack Homepage

Solange der Vorrat reicht, können auf der Compu-Shack Homepage `www.technik-News.de` unter `Publikationen` kostenlos Demos und Trials auf Original Novell CDs abgerufen werden. Dort finden Sie auch Datenblätter zu Novell und Compu-Shack Produkten im Acrobat Format zum Download.
Im Moment sind folgende CDs verfügbar:

ManageWise 2.6,
90 Tage Trial Version

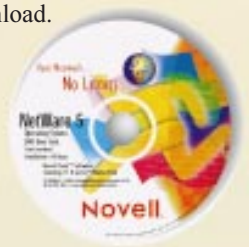
Z.E.N. works Starter Pack

NDS for NT 2.0,
Time Trial bis 31.08.1999

GroupWise 5.5 Multilingual,
3-User Demo-Version

NetWare SmallBusiness 4.2,
25-User Time Trial
bis 30.06.99

NetWare 5,
500 User 60-Tage
Trial-Version



BorderManager Enterprise Edition 3,
60 Tage Trial Version

Jahr 2000 Check für Novell Netzwerke

SEMINARE

Neue Windows 2000 Kurse

MS 1561

Planning and Implementing Microsoft Windows 2000 Directory Services
Planung, Installation und Support einer Directory Service Infrastruktur, inklusive ONS, Active Directory und Microsoft Exchange 5.5 Integration.

MS 1561

Planning and Implementing Microsoft Windows 2000 Networking Services
Planung, Installation, und Support einer Microsoft Windows 2000 Netzwerk Infrastruktur, inklusive Virtual Private Networks (VPNs), Routing Services, und Network Security Services.

MS 1563

Deploying Microsoft Windows 2000 Professional in a Microsoft Windows 20000 Server Network
Planung und Implementierung für Client Computer mit Microsoft Windows 2000 Professional arbeiten, inklusive Applications, User Enviroment Restrictions und Mobile User Suppport. Ein Überblick zu Unterlage 1560 Upgrading Support Skills from Microsoft Windows NT 4.0 to Microsoft Windows 2000. Kurs 1560 wird die Voraussetzung sein für die Kurse 1561, 1562, oder 1563

Voraussetzungen
Das Training richtet sich an erfahrene Windows NT 4.0 Spezialisten, NT Kenntnisse bzw. Trainererfahrung sind unbedingt notwendig. Idealerweise verfügen Sie über einen aktuellen MCSE in Windows NT 4.0 (TCP/IP [Examen Nr. 70-059), Exchange [Examen Nr. 70.081])
.

Build with BayStack

Workshop von Compu-Shack und Nortel Networks

Die Unified Network-Lösungen von Nortel Networks beruhen auf IP-optimierten Technologien, die mit der Integration von Sprache, Daten und Video neue Maßstäbe setzen, in Leistung, Zuverlässigkeit und Verfügbarkeit. Nortel Networks und Compu-Shack veranstalten zu diesem Thema im Juni eine gemeinsame Roadshow. Die bundesweiten Workshops "Build with BayStack" stellen aktuelle Lösungsmöglichkeiten mit der BayStack Familie und dem Accelar Gigabit/ IP-Routing Switch vor.

Mit der 10/100 Autosensing Switching Technologie in den BayStack Serien 350 und 450 hat Nortel neue Maßstäbe im Switching Bereich gesetzt und bietet mit der Bay-Stack Familie skalierbare Lösungen für mittelständische Unternehmen an. Zukünftige Erweiterungen der Bay-Stack Familie werden es ermöglichen, schrittweise Sprach-Daten-Integra-tion anzubieten. In Kombination mit der erfolgreichsten Gigabit Ethernet/Layer 3 Switch Familie Accelar sind gerade mittlere Unternehmen in der Lage, Gigabit Ethernet/Layer 3 Lö-sungen skalierbar zu gestalten, die den Weg zu Unified Networks bereiten.

Zukunftslösungen

Der Workshop "Build with BayStack" vermittelt einen aktuellen Überblick über die Lösungsmöglichkeiten der BayStack Familie. Außerdem werden die Einsatzmöglichkeiten des Accelar Gigabit/IP Routing-Switch erläutert. Lernen Sie die Netzwerke der Zukunft zu bauen. Die Termine sind am 2.6.99 in Köln/Düsseldorf, am 7.6.99 in München, am 8.6.99 in Berlin/Leipzig, am 10.6.99 in Hamburg, am 15.6.99 in Stuttgart und am 16.6.99in Frankfurt. Die Veranstaltungen beginnen um 12.30 Uhr mit einem Mittags-Snack und enden um 18.00 Uhr mit einer Abschlußdiskussion. Anschließend gibt es ein gemeinsames Abendessen.

Ausgewählte Termine

02.06.99	Workshop "Build with BayStack"	Köln/Düsseldorf
06.-09.06.99	Microsoft Tech Ed Europe 99	Amsterdam
07.06.99	Workshop "Build with BayStack"	München
08.06.99	Workshop "Build with BayStack"	Berlin/Leipzig
08.-11.06.99	CAT ´99	Stuttgart
10.06.99	Workshop "Build with BayStack"	Hamburg
15.-17.06.99	Voice Germany	Köln
15.06.99	Workshop "Build with BayStack"	Stuttgart
16.06.99	Workshop "Build with BayStack"	Frankfurt
23.- 25.09.99	InterGeo ´99	Wiesbaden
05.-07.10.99	exponet 99	Düsseldorf
24.02.-01.03.00	CeBIT 2000	Hannover

Vorschau Technik NEWS

N°07

Thema des Monats

Saver Server

Datensicherung mit VINCA

Von Thomas Martin

Wie sichert ein großes Unternehmen seine Datenserver? In unserem Schwerpunkt berichten wir über ein Praxisbeispiel, in dem die Entscheidung für ein sekundäres Rechenzentrum mit Glasfaseranbindung fiel. Welche Produkte unterstützen eine Spiegelung der Daten und erleichtern das Backup großer Datenmengen? Die Auswahl fiel auf den Vinca Standbyserver für IntraNeware. Wir berichten, welche Voraussetzungen für den Einsatz vorliegen müssen, geben Hinweise zu Installation, Troubleshooting, Performance-Daten und Tuning, nennen die notwendigen Patches, haben Tips zur Konfiguration und zum Management der Applikation via SNMP zusammengetragen und zeigen Überwachungs-Möglichkeiten durch die Auswertung und Email-Weiterleitung von SNMP-Traps mit der CS-Trapconsole.

Praxis spezial:

Operation 2000

Windows Scrip Host, Teil 1